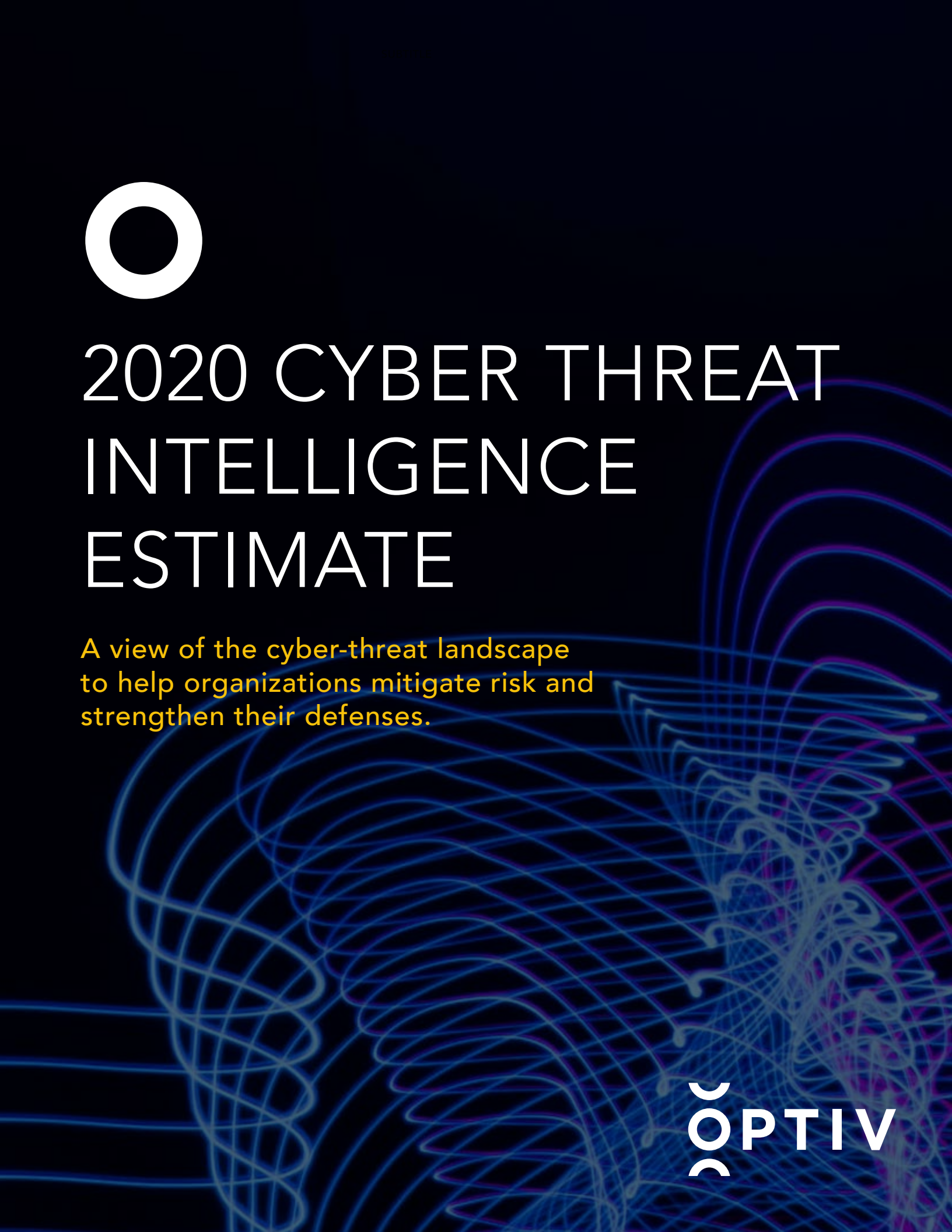
2020 CYBER THREAT INTELLIGENCE ESTIMATE

A view of the cyber-threat landscape to help organizations mitigate risk and strengthen their defenses.



OPTIV

Table of Contents

Introduction

The threat landscape is more intense and more complex than ever before.

COVID-19 and the resulting shift for many of us to work-from-home has increased opportunities for threat actors and also increased the burden on cybersecurity providers. Many businesses now rely more heavily on third-party vendors, as well, and this amplifies the risks that already existed for companies contending with identity and data management challenges, privacy regulations and the Internet of Things.

It is vital for business leaders to understand these developments and the consequent need to protect a larger, more fluid attack surface that is more vulnerable to both internal and external threats than previously was the case.

Beyond that, threat actors also constantly develop and acquire new tools, techniques and procedures, and refine existing ones, in their efforts to identify and exploit vulnerabilities. The best way to protect effectively against malicious activity is to take a comprehensive, integrated and managed approach to cybersecurity, a key component of which is up-to-date threat intelligence. In fact, the most efficient and effective threat countermeasures are based on a detailed understanding of the ever-evolving threat landscape.

This Cyber Threat Intelligence Estimate summarizes key threat activities, threat actors and topics crucial to data breach prevention. It also provides recommendations that business leaders and security practitioners should consider as they make decisions about cybersecurity programs and investments, as well as risk management.

General David Petraeus,
US Army (Retired),
Partner, KKR and Chairman,
KKR Global Institute,
Optiv Board Member

Executive Summary

The 2020 Cyber Threat Intelligence Estimate (CTIE) is inspired by national intelligence estimates, which are analytic reports produced by the intelligence community of the United States for consumption by Congress.

Evolving technology, threat actors and regulations require security leaders and security practitioners to be familiar with their own environment and assets and stay abreast of the latest global threat trends. This report comprises contributions from Optiv's Global Threat Intelligence Center (gTIC); VMware Carbon Black; Digital Shadows; Palo Alto Networks global threat intelligence team, Unit 42; and SailPoint.

This CTIE summarizes the following information:

Vertical Industry Breach Highlights

9

Attack Tools, Techniques and Procedures

12

Hybrid Threat Actors

22

Data Breaches

30

Dark Web Practices

38

Additionally, a special section on COVID-19 offers insights into security concerns as well as actions that business leaders can take to bolster cybersecurity.

By applying the best-practice recommendations provided in the CTIE, decision-makers and influencers can strengthen their cybersecurity strategies and operations. For organizations that collect and analyze their own threat intelligence, the intelligence assembled in the CTIE can validate and augment their findings.

COVID-19 Updates

The COVID-19 pandemic has had and will likely continue to have profound, long-lasting effects on companies and people. The following insights and guidance may be useful to business leaders whose employees are working from home. Remote access support via phone, chats and video create new and different vulnerabilities. This massive expansion of the attack surface is a necessity for business continuity, but it comes with security and risk concerns.

Workers often are unaware of threats, further increasing risk.

> Since January 2020, **more than 4,000** coronavirus-themed web domains have popped up, and around **5% were suspicious and 3% malicious**.[1]

Digital Shadows blogs describe phishing and social engineering scams, sale of fraudulent or counterfeit goods and COVID-19 cures, and general misinformation.

Many businesses have turned to third-party vendors – for collaboration solutions, for example – to support productivity. Digital Shadows analysts identified potential third-party risks:

- **Operational risk** involves potential losses resulting from inadequate or failed procedures, systems or policies.
- **Transactional risk** involves potential losses due to problems with a service and/or its delivery.
- **Compliance and regulatory risk** result from third-party security breaches.

During these uncertain times, an enterprise's security roadmap and objectives remain the best framework within which to make decisions. Existing cybersecurity principles apply now more than ever, especially for industries at high risk for cyber attacks.

IMPACTS

Organizations and industries most crucial to the COVID-19 response, or those already affected by the economic fallout caused by the pandemic, are likely most at risk of being targeted by cyber-threat actors. Digital Shadows analysts point to warnings from governmental and intergovernmental agencies, directed particularly to healthcare businesses and manufacturers of critical medical equipment and personal protective equipment, stating that a disruptive cyber attack will amplify their struggles.

The VMware Carbon Black team analyzed financial services firms and discovered that the cybercriminal community took advantage of COVID-19 in tandem with the news cycle, escalating their coordinated criminal conspiracies. Everyone should pay close attention to these threat actors and thwart their goal: hijacking digital transformation efforts via island hopping.

STRATEGIES

Optiv cybersecurity experts find that employers are pursuing three basic strategies to combat COVID-19:

» Expand existing access

» Create alternate access methods

» Redesign infrastructure

Fortunately, providing expanded access services for employees and customers dovetails with common organizational priorities:

» Moving workloads to the cloud

» Migrating to software as-a-service (SaaS) applications

» Retooling identity governance

» Enabling mobility/bring your own device (BYOD)

» Applying Zero Trust access methods

OTHER ACTIONS YOU CAN TAKE TO MINIMIZE THE IMPACT OF COVID-19

» **Provide security awareness training.** Make it easy for workers to find documentation about remote access and how to be safe online. Publish a list of approved collaboration tools for chat and online meetings. Supply guidance on which applications can be accessed remotely.

» **Deploy and update endpoint security agents.** Validate and publish the steps to enroll your remote endpoint security agent. Implement host validation checks to ensure a minimum standard is met before allowing access to sensitive information. And, determine the level of access that will be permitted for personal devices.

» **Manage user identities properly, including accurate, accessible directory services.** Leverage a single-sign-on (SSO) dashboard for application distribution and use multifactor authentication wherever possible. Enhance and expand monitoring and reporting on access to sensitive information.

» **Include SecOps management in business-line decision planning related to remote workforce enablement.** Your SecOps/cybersecurity teams need to stay on top of changes in traffic flows, peak operating times and new sources of telemetry to incorporate into monitoring tools. A tiger team can best implement the acquisition and monitoring of new telemetry for net-new applications and access methods. Be prepared to coach employees on how working from home will change usual business practices and behavioral monitoring systems.

» **Vet suppliers thoroughly.** Make sure security practices match your requirements and monitor third-party applications so incidents can be tracked and resolved.

As you decide how your business will operate during this fluid situation, keep cybersecurity top of mind as you respond to the increased threat level. COVID-19 checklists are available from Optiv upon request.

Data Gathering and Analysis

Security analysts gather, weigh and synthesize data sources to prepare the intelligence analysis that appears in the CTIE. Some of the data is circumstantial, and it is up to the analysts to find multiple, corroborating intelligence data points to assemble a clear picture that describes the threat landscape. Experts from the contributing companies collect cyber-activity statistics from thousands of clients, and the data is summarized here so you can easily understand key activities, events and trends.

THREAT TRENDS

A comparison of 2018 and 2019 threat activity observed by Optiv reveals patterns that indicate shifting trends. In this comparison, a threat is any event that may cause a security incident.

16% fewer threats in 2019 than 2018 in total on average

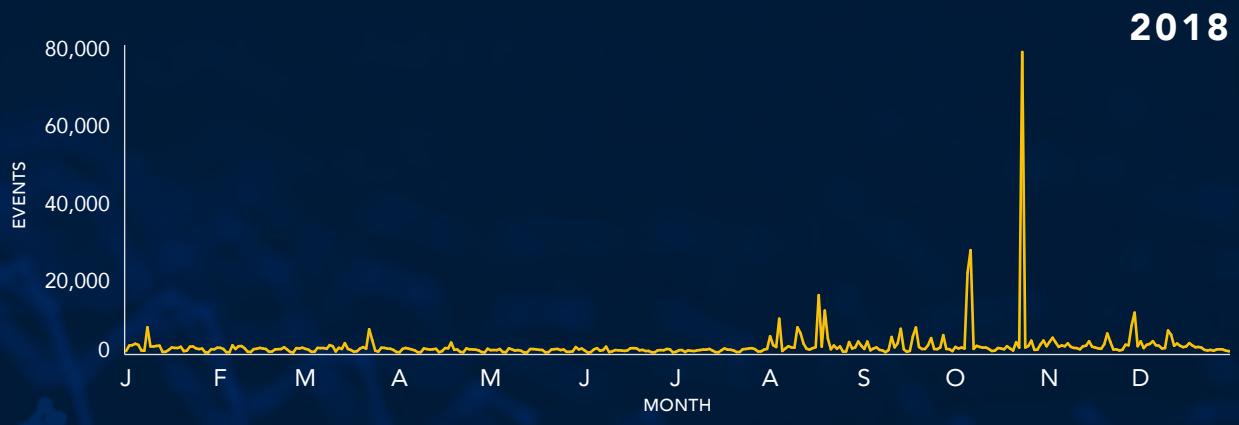


Figure 1 - Observed threat activity in 2018 (Optiv)

Figure 2 - Observed threat activity in 2019 (Optiv)

At the end of 2018, overall threat activity gradually increased before dropping off for a few months. This trend continued throughout 2019 in two large cycles, each made up of two smaller cycles. On a standard fiscal year quarterly basis, aspects of the threat landscape reset and then gradually started to climb. Cumulative highs at the beginning and end of the year point to the idea that threats will continue to occur around specific events and timing-oriented attack patterns to maximize damage. In total, the average threats per day in 2019 appear to be about 16% lower than the threats in 2018.

PHISHING AND BRAND MISUSE, INFRASTRUCTURE AND DATA LEAKAGE INCIDENTS

As organizations and their brands continue to grow, their attack surfaces also grow. Attackers are increasingly targeting and impersonating organizations across all channels. Digital Shadows classifies this activity into three main incident categories: phishing and brand misuse, infrastructure and data leakage. Phishing and brand misuse include malicious and impersonating web domains, as well as spoof social media profiles. Infrastructure includes domain certificate issues and port exposures. Data leakage covers the exposure of sensitive documents, customer details and code on unwanted or unintended sources.

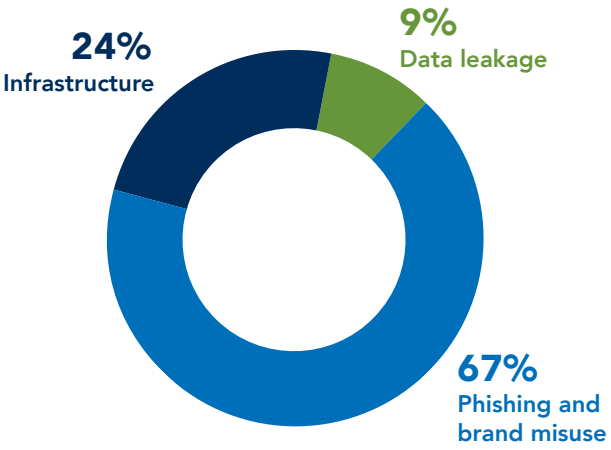


Figure 3 - Breakdown of 2019 incidents (Digital Shadows).

DATA LEAKAGE ALERTS

Data leakage alerts include unmarked documents, customer details, protectively marked documents, technical leakage and internally marked documents.

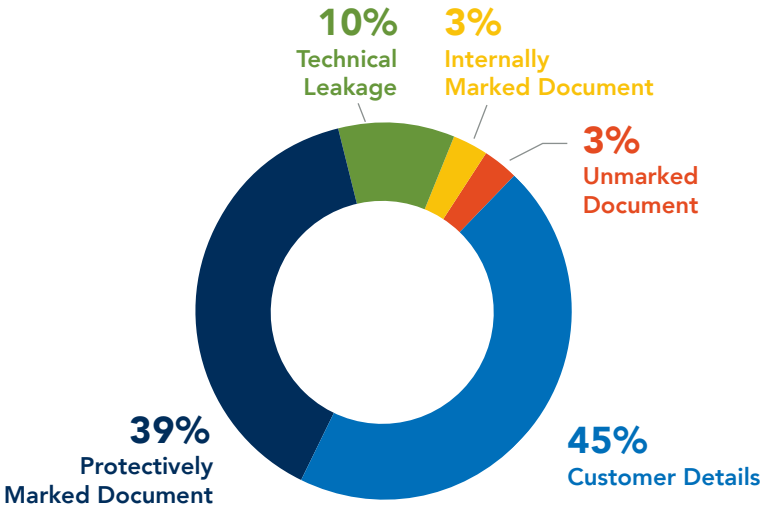


Figure 4 - Breakdown of 2019 data leakage alerts (Digital Shadows).

VERTICAL INDUSTRY DATA

For all incidents reported by Digital Shadows, the majority, 66%, belong to organizations in the technology and financial services sectors. These include alerts for impersonating domains, spoof social media profiles, data breaches and credential exposure, and exposed documents.

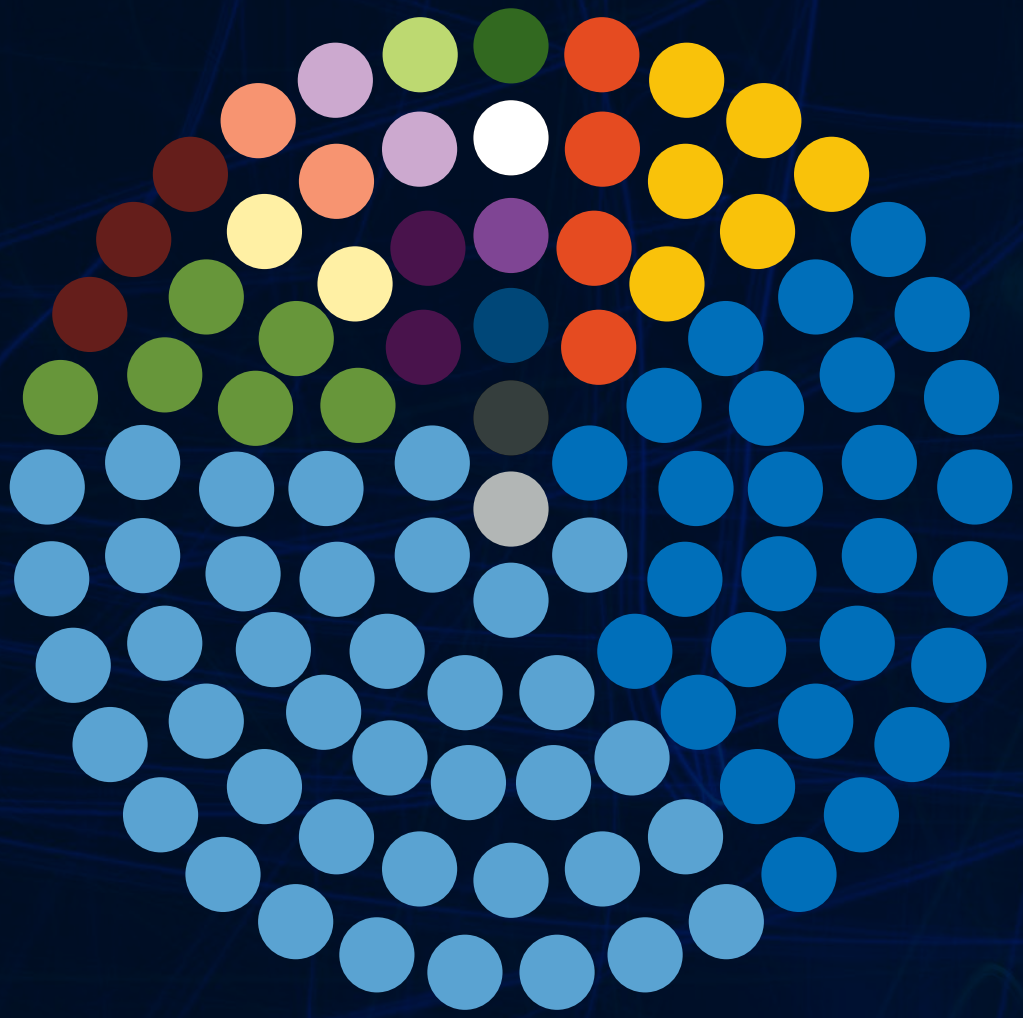


Figure 5 - 2019 Alerts by Vertical (Digital Shadows).

66% of incidents belong to organizations in the **technology and financial services** sectors

LEGEND

- TECHNOLOGY
- FINANCIAL SERVICES
- OTHER
- HEALTHCARE
- RETAIL
- OIL AND GAS
- TRAVEL AND LEISURE
- UTILITIES
- EDUCATION
- FOOD AND BEVERAGE
- INSURANCE
- AUTOMOBILES AND PARTS
- GOVERNMENT
- PERSONAL AND HOUSEHOLD GOALS
- EQUITY/NON-EQUITY INVESTMENT INSTRUMENTS
- LEGAL SERVICES
- BASIC RESOURCES

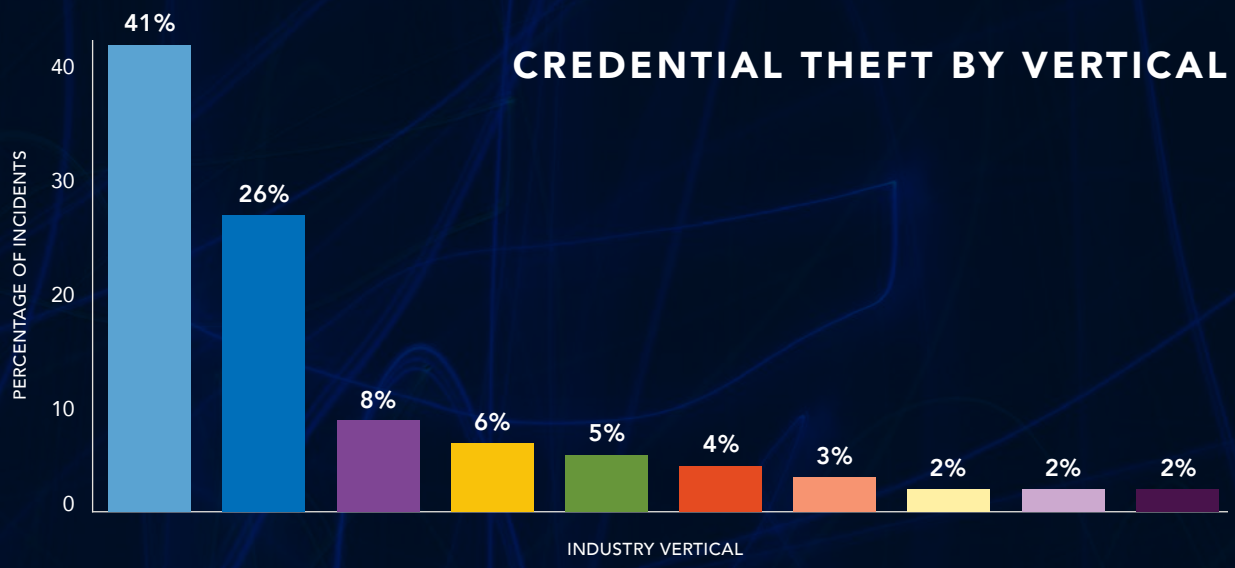


Figure 6 - 2019 credentials by vertical (Digital Shadows).

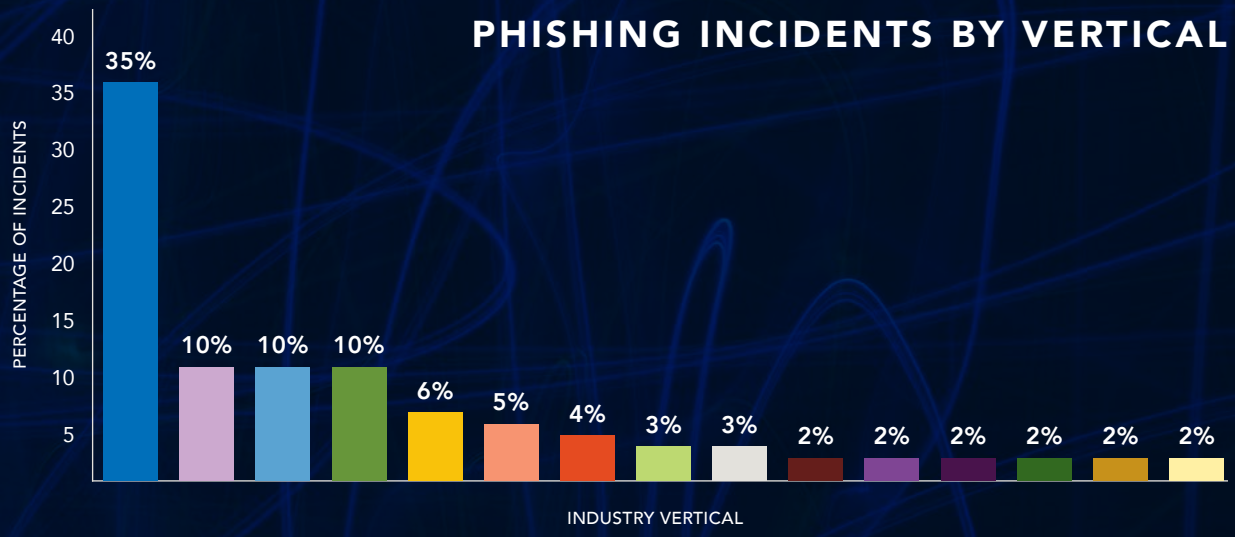


Figure 6 - 2019 phishing by vertical (Digital Shadows).

LEGEND

- TECHNOLOGY
- FINANCIAL SERVICES
- OTHER
- HEALTHCARE
- RETAIL
- OIL AND GAS
- TRAVEL AND LEISURE
- UTILITIES
- EDUCATION
- FOOD AND BEVERAGE
- INSURANCE
- AUTOMOBILES AND PARTS
- GOVERNMENT
- MEDIA
- EQUITY/NON-EQUITY INVESTMENT INSTRUMENTS

Vertical Industry Breach Highlights

Industries at high risk from certain vulnerabilities and threats are discussed below. Optiv's threat actor risk metric system[2] can help you assess risk and develop appropriate countermeasures.

Companies across industries increased their risky use of Secure Shell (SSH), Remote Desktop Protocol (RDP) and Transport Layer Security (TLS). According to Palo Alto Networks analysts, attackers target SSH when it is configured to use password authentication, creating a low barrier to entry. To thwart these attacks, use public key authentication (RSA, ECDSA or Ed25519 key pairs) for all SSH-enabled systems.

RDP operates over port 3389 to enable remote administration of Windows environments. RDP is frequently used as an initial vector for ransomware. Instead of exposing RDP to the public internet, use alternatives such as Virtual Desktop Infrastructure (VDI) or virtual private networks (VPNs) that provide connectivity without exposing public IPs.

TLS is a protocol that provides authentication, privacy and data integrity between communicating applications. There are several vulnerabilities in older versions of TLS. Several certificate authorities have largely deprecated versions 1.0 and 1.1, making it advisable for organizations to support only v1.2 and 1.3.

For cloud operations, a Zero Trust approach is the best practice, regardless of industry type. Cloud service providers are not responsible for managing an organization's cyber risk. Organizations using the cloud must protect their applications and data, but unauthorized access and inconsistent security policies make this challenging. Also, organizations typically use more than one cloud platform. **Zero Trust frameworks are built on the notion of "never trust, always verify,"** meaning that no access is permitted without identification. However, identification alone is not sufficient. After access is established, traffic flow should be inspected continuously.

HEALTHCARE

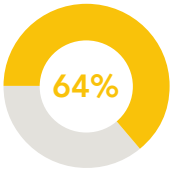
Palo Alto Networks analysts conclude that risk for healthcare companies is elevated because Internet of Things (IoT) device security has declined, leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques. Analyst research reveals these key IoT concerns:

- **Outdated software.** 83% of medical imaging devices run on unsupported operating systems – a 56% jump from 2018 as a result of the Windows® 7 operating system reaching its end of life. Just over half (51%) of threats involved imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices. This general decline in security posture opens the door to new attacks, such as cryptojacking, and brings back threats like Conficker.
- **Poor network hygiene.** 72% of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network. 41% of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices to exploit known weaknesses. Attacks are shifting from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data and monetary profit via ransomware.
- **Inadequate security function.** Biomedical engineers who maintain medical devices often lack the training and resources to follow IT security best practices: password rules, secure password storage and maintaining up-to-date patches.

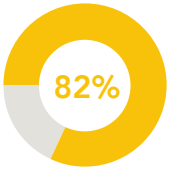
FINANCIAL

In recent months, as COVID-19 disordered many businesses, VMware Carbon Black analysts observed a 148% increase in ransomware attacks and a 238% increase in attacks against the financial sector. The research shows:

of surveyed banks said they saw an increase in cyber attacks over the past 12 months, marking a 13% increase over 2019.



of surveyed financial institutions reported increased attempts of attempted wire fraud transfer, a 17% increase over 2019.



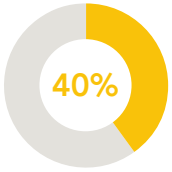
of surveyed financial institutions said cybercriminals have become more sophisticated, leveraging highly targeted social engineering attacks, advanced TTPs for hiding malicious activity, and exploiting weaknesses in people, processes and technology to gain a foothold and persist in the network enabling the ability to transfer funds and exfiltrate sensitive data.

> Analysts observed a **148% increase in ransomware** attacks and a **238% increase in attacks overall**

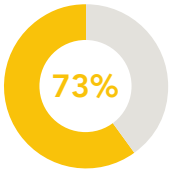
RETAIL/HOSPITALITY

Retail was heavily targeted during the past year by cyber-based attacks. The most common observed malware families included Emotet, Obfuse and Kryptik. E-commerce sites are favorite targets for cybercriminals that commonly leverage skimming scripts such as Magecart to scrape and exfiltrate payment card information. Criminal threat actors commonly attempt to spoof a legitimate vendor or exploit a vulnerability on the e-commerce vendors' payment page to inject a crafted JavaScript skimmer.

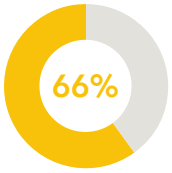
VMware Carbon Black research reveals:



of retailers lost revenue in 2019 due to cyber attacks



saw increasingly sophisticated cyber attacks as the year progressed, and 33% of these organizations experienced an island-hopping attack

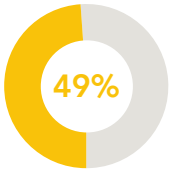


of the surveyed organizations experienced a ransomware attack[3]

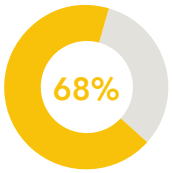
MANUFACTURING

According to a recent study, 40% of manufacturers were affected by a cyber incident.[4] Verizon provides additional insights:

of manufacturing attacks were made up of internal actors



of organizations report having credentials compromised



of documented cases were financially motivated and **27% were espionage related**[5]

ENERGY/UTILITIES

Energy and utilities companies were affected by some of the most high-profile cyber attacks between 2015 and 2018. In March 2019, a Utah-based utility company became the first American energy company to see grid operations get disrupted by a cyber attack.[6] Dragos and E-ISAC observed an increase in scans of U.S. and East Asia-based industrial control systems (ICS) by the XENOTIME threat actor.

RECOMMENDATIONS

- ☑ Implement network segmentation to **limit the attack surface** available to an insider threat
- ☑ Apply **multi-factor authentication**
- ☑ Develop system access policies following the **least-privilege principle**
- ☑ Implement patch management to **ensure systems are updated** to the latest version

Attack Tools, Techniques and Procedures

Tools, techniques and procedures (TTPs) are common topics in threat intelligence circles because they are some of the simpler aspects to study. Threat actors use TTPs – which describe the "how" and "what" – to carry out their attacks. The correlation and analysis of TTPs help analysts figure out the "who" and "why." Important TTPs involve cryptomining, IoT attack methods, cyber espionage and malware.

CRYPTOMINING

Palo Alto Networks analysts found that nearly 9% of cloud organizations showed signs of connecting to, and likely performing, mining operations via public Monero (XMR) mining pools. Public mining pools are systems or networks that coordinate, manage and distribute mining operations. Remote systems connect to these pools to receive mining instructions and, upon completion of the operations, receive a share of the resulting financial proceeds.

Nearly 60% of all public XMR mining network connections to XMR pools are located within the United States. Mining operations can evade geographic blacklisting or whitelisting based solely on country or region criteria. They take place often over ports such as 80 and 443, which are meant to avoid corporate firewall rules.

Frequently used tools include:

» **Rocke.** This tool has evolved cyber operations beyond cryptomining with another tool called Godlua, which performs proxy Lua (a programming language designed primarily for embedded use in applications) scripting operations and various shell operations within cloud infrastructure. Network connections to known Rocke infrastructure trended downward, in part because cloud environments are less reliant on native cloud service provider network controls.

» **8220 Mining Group.** The tell-tale signs of 8220 operations within network environments involve the use of port 8220. While port 8220 is an uncommon port for default networked environments, it is possible for port 8220 to be used for custom purposes. Researchers paired network connections like PE-Miner and XMRig from organizations with connections over port 3333, which is a commonly used port by 8220 and known to be used by cryptomining software. Based on known 8220 indicators of compromise (IOCs), Palo Alto Networks analysts found that 21% of cloud organizations had network connections that appeared to have 8220 signatures

The pattern of cloud system connections over ports 3333 and 8220 to external systems is suspicious because a single destination system was being connected to using two separate ports. And, it is suspicious for destination IP addresses used in the connections not to be routed through DNS name resolutions and instead called directly through their IP addresses.

» **Pacha.** Pacha competes with Rocke for cryptocurrency mining in the cloud, but activities in 2019 declined significantly. 93% of Pacha cryptocurrency traffic was destined for China, although the specific types of network operations being performed are unknown.

RECOMMENDATIONS

- ☑ **Use Layer 7 packet inspection** signatures via virtual next-generation firewalls
- ☑ **Integrate** virtual network traffic **inspection tools**
- ☑ **Apply virtual next-generation firewalls** (NGFWs) to block connections to known Rocke infrastructure
- ☑ **Block 8220 communications** by preventing communications with known malicious IP addresses

INTERNET OF THINGS

IoT adoption grew to an estimated 4.8 billion devices, up 22.5% from the end of 2018.[7] Palo Alto Networks analysts found that 98% of IoT traffic is unencrypted, exposing personal and confidential data on the network and that 57% of IoT devices are vulnerable to medium- or high-severity attacks. IoT offers low-hanging fruit due to the vulnerabilities created by low patch levels and aging operational technology (OT) protocols.

According to Optiv IoT experts, IoT cybersecurity received more attention during the past year, in part because ownership shifted to chief information security officers (CISOs). In the past, IoT security belonged to several groups, resulting in isolated initiatives. With greater responsibility and budget control in the hands of CISOs, they can be stronger IoT champions.

An immediate enterprise priority is a unified incident response (IR) platform that incorporates both IT and OT. The lack of a unified IR platform continues to hamstring business continuity and business recovery efforts. Some companies lump IT and OT into the IoT bucket, but OT goes beyond the usual security concerns to include product/manufacturing protection requirements. Attackers tunnel through from IT to OT using paths of least resistance. Once inside, they can linger and eventually access entire environments depending on security maturity.

Some decision makers are pursuing Zero Trust fundamentals to improve IoT cybersecurity. Device visibility received a boost from new tools capable of pulling out vulnerability data. Segmentation gained momentum, but it was limited due to cost, complexity and resource constraints. An alternative is cloaking – a duplicate, disguised network that allows authorized traffic.

Use Cases

Ryuk Ransomware

The Ryuk ransomware **took down a United States Coast Guard facility for more than 30 hours** in late 2019. The point of entry was a malicious email sent to an employee. After the employee clicked on a link, a threat actor accessed and encrypted critical IT network files, blocking staff access to the information. The virus spread throughout the facility, also impacting industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations.[8] Ryuk attackers, which reportedly target firms with annual revenue between $500 million and $1 billion, also targeted oil and gas companies, including Mexico's Pemex.[9]

Urgent/11

Urgent/11 is a suite of network protocol bugs that creates vulnerabilities in TCP/IP stacks by allowing devices to connect to networks like the internet. The code has been around for many years, and the bugs exist in far more platforms than originally believed. **Always-on devices common in industrial control settings and the healthcare industry** are particularly vulnerable to attacks or takeovers. At least seven affected operating systems run in countless IoT devices.[10]

Top IoT Attacker Methods

The Palo Alto Networks analysts scrutinized cross-industry research and identified these key methods used by attackers to compromise IoT:

» **Exploits target device vulnerabilities.** IoT devices are used as stepping stones in lateral movement to attack other systems on a network. Attacker activities include network scans, IP scans, port scans and vulnerability scans on networks that attempt to identify potential next-step targets.

» **Password attacks.** These attacks are fueled by default, manufacturer-set passwords, poor password security practices and operational misalignment. For example, passwords chosen by OT staff are not in line with the more advanced password policies and password management practices used by IT. California's SB-327 IoT law now prohibits the use of default credentials, which will help reduce password attacks.

» **Unclosed backdoors.** WannaCry ransomware attacks spread through backdoors left open by previous DoublePulsar malware infections. The use of unpatchable devices, such as those running Windows 7, allow these two-stage attacks to continue happening.

» **Unsegmented networks.** WannaCry cases in healthcare spreads in mixed networks with devices such as PCs, scanners and nuclear imaging devices. With strong self-propagation and infection capability, WannaCry cross-infects devices throughout IoT and IT.

» **Botnet attacks.** The Mirai malware turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale attacks. Primary targets are online consumer devices such as IP cameras and home routers. Mirai has grown into a framework to which developers can add new device exploits as new variants.

RECOMMENDATIONS

☑ **Develop an IoT security strategy** that encompasses the entire IoT lifecycle and all IoT devices

☑ **Discover IoT devices** on your network

☑ **Patch printers** and other easily patchable devices

☑ **Segment IoT devices across VLANs** – micro-segmentation is preferred

☑ Implement active **around-the-clock monitoring**.

☑ Use a **vulnerability management process** that encompasses:

- » Asset discovery
- » Identification of vulnerabilities in the assets
- » Threat intelligence to prioritize vulnerabilities
- » Patching, configuration management and isolation as remediation methods

2019 NOTABLE IoT ATTACKS

SEPTEMBER 2019

Palo Alto Networks analysts discovered an **updated Gafgyt variant attempting to infect IoT devices**, specifically small office/home wireless routers of certain commercial brands.

DECEMBER 2019

Palo Alto Networks analysts discovered a **new variant of the Muhstik botnet** that adds a scanner to attack Tomato routers by web authentication brute forcing. Muhstik, which **has a wormlike self-propagating capability to infect Linux servers and IoT devices**, mainly launches cryptocurrency mining and DDoS attacks with IoT bots to earn profit.

CYBER ESPIONAGE

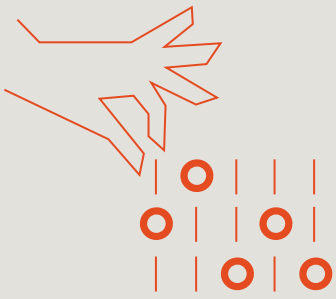
Optiv's gTIC followed cyber espionage, which is cyber activity directed at private and public sector entities with the aim of stealing sensitive or classified data or intellectual property to gain a competitive advantage over a rival organization or country. Threat actors engaged in cyber espionage are sophisticated and often fall under the classification of advanced persistent threats (APTs). Depending on their target, they can exploit a range of vectors to establish a foothold within a target system. These attacks are often preceded by reconnaissance activity. The ramifications of espionage include loss of competitive advantage, sabotage and political instability.

Tools

Threat actors often leverage both in-house and publicly available hacker tools common among many threat groups. This not only frees up time and resources but also makes post-exploitation analysis and attribution more difficult – adding to the attackers' level of obfuscation.

Espionage attacks do not differ much from financially motivated attacks, but they can span a longer timeframe. State-hosted espionage operations are commonly supported by a much larger and sophisticated infrastructure than those used by criminal actors. Some commonly leveraged public tools include:

- **PsExec.** This tool is part of Microsoft's Sysinternals. It enables system administrators to remotely access and manage their systems over the Server Message Block (SMB) protocol, TCP port 445. The open-source penetration tool Metasploit specifically contains a PsExec exploit module that allows an attacker to conduct remote code execution on a targeted machine.
- **Mimikatz.** An offensive security tool, Mimikatz can be used at the post-exploitation phase of an attack. Its functionality encompasses password dumping from memory, PINs, hashes and Kerberos tickets. This tool works by exploiting Windows single-sign-on (SSO) procedures. Successful exploitation can enable other attacks including pass-the-hash and Golden Ticket attacks.
- **X-Agent.** This modular backdoor is leveraged by APT28, a Russian state-linked espionage group with ties to GRU, Russia's military intelligence organization. Also called CHOPSTICK, X-Agent functionality focuses on information gathering and includes capabilities such as logging keystrokes, transmitting remote files, taking screenshots and modifying registries.



Turla Hijacks APT34 Tools

In October 2019, the United Kingdom's National Cyber Security Centre (NCSC) and the United States' National Security Agency (NSA) issued a joint advisory. It stated that the Russian state-associated threat actor Turla used tools linked to the Iranian threat actor APT34. This included the Neuron and Nautilus tools designed to target mail servers and web servers on Windows. Turla used Neuron and Nautilus to target a range of victims, including a cluster of Middle Eastern organizations.

- **Empire.** An open-source post-exploitation framework, Empire can operate cross-platform. It is used by advanced persistent threat actors including APT33, APT19, FIN10 and Turla. Empire can run PowerShell agents without powershell.exe along with a range of post-exploitation modules geared to logging keystrokes, network detection evasion and containing Mimikatz. Additionally, Empire's network traffic was asynchronous and blended in with normal network traffic. Development of Empire ceased in mid-2019.
- **netstat.** This operating system utility is used to display TCP connections, network connections and listening ports common within Windows, Linux and UNIX.
- **Cobalt Strike.** A commercially available penetration testing tool, Cobalt Strike has been adopted by several espionage threat actors. These include APT29, APT17 and CopyKittens. Its full range of post-exploitation functions present cyber-espionage actors with a convenient framework.

RECOMMENDATIONS

- ☑ Enforce a security policy that covers **cyber-based, insider and physical-based threats** to stop cyber-espionage threat actors that go to great lengths to access their targets
- ☑ Ensure operating systems, software and firmware are patched to the latest updates with **patch management that maintains automatic updates**
- ☑ Implement **multi-factor authentication**

MALWARE: KRYPTIK, OBFUSE AND EMOTET

VMware Carbon Black analysts provided insights into Kryptik, Obfuse and Emotet. This malware is often used in long, complex campaigns for which the end goal is to leverage native operating system tools to remain invisible or gain a foothold in one system (sometimes a supply chain partner) to island hop to a larger, more lucrative target.

The Kryptik trojan attempts to target victim machines via nefarious installers. It then attempts to acquire admin rights to make registry modifications, allowing it to execute each time a Windows machine boots. Kryptik can be persistent and, without appropriate visibility, can be difficult to detect as it attempts to delete its executable file after running.

As noted by a threat profile from the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC): "[The Kryptik trojan] queries the Windows registry for the .ini or .dat file paths. It also queries registry subkeys for the actual host, username and password related to the specific FTP client application. Kryptik searches the registry, querying for both ftpIniName and InstallDir that hold the wcx_ftp.ini file. The trojan can recover many common FTP clients, email clients, file browsers and file manager programs. Kryptik also can update itself and remotely download new versions."[11]

Obfuse is a trojan virus designed to steal confidential data stored on a system. It is delivered through porn websites, free online games, peer-to-peer file sharing, misleading ads, free third-party software and spam email attachments. Difficult to detect and remove, Obfuse can disable antivirus software, redirect browsers, slow system speed, freeze programs and pay repeat visits after creating new malicious registry keys.

Emotet, a family of banking malware, has been around since at least 2014. Attackers continue to leverage variants of Emotet and are becoming increasingly shrewd in the techniques they employ to deliver the malware onto an infected system. Researchers using managed hunting services observed a spike in the adaptation to existing methods leveraging PowerShell. Attackers encrypted the URLs of the command and control (C2) systems used to host the second-stage payload.

Further, several attacks originated from phishing campaigns that leverage Microsoft Office Word documents with obfuscated VBScripts using PowerShell and the ConvertTo-SecureString cmdlet, which in the later stages is used to decrypt the C2(s) and associated logic. This represents an evolution of current macro attack techniques – these types of cmdlets are not typically associated with phishing campaigns.

A three-part Palo Alto Networks blog series focuses on static analysis of PowerShell scripts and a platform-independent Python script to carry out the task. The author studied approximately **5,000 PowerShell scripts** and **describes behavioral profiling, common obfuscation, methods of hiding data** within PowerShell scripts and a scoring system to assess risk.

RECOMMENDATIONS

- ☑ **Install next-generation antivirus coupled with endpoint detection** and response (EDR) and micro-segmentation to thwart malware attacks
- ☑ **Implement techniques within Microsoft environment** such as Microsoft Just Enough Administration (JEA) to allow delegated control; Remove use of older PowerShell 2.0, which has been deprecated, and enable PowerShell transcription logging and Script Block Logging

MALWARE: RANSOMWARE

Optiv's gTIC team (using the ThreatDNA platform) found that ransomware was an influential topic throughout the past year in circles outside of the information security industry.

> Numerous industry leaders and organizations saw a **drastic increase in ransomware activity,** as reported in the news and incident response reports.

Many ransomware concepts can be explained by reviewing what is known about the MITRE ATT&CK® for Enterprise patterns used by most ransomware families. Knowing more about how ransomware works will help identify and address vulnerabilities.

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done to extract monetary compensation from a victim in exchange for decryption or a decryption key to render data permanently inaccessible in cases where the key is not saved or transmitted.

In the case of ransomware, common user files like Microsoft Office documents, PDFs, images, videos, audio, text and source code files are typically encrypted. In some cases, adversaries may encrypt critical system files, disk partitions and the master boot record (MBR). To maximize the impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like valid accounts.

Threat actors may also stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services can inhibit or halt responses to an incident or aid the adversary's overall objectives to cause damage to the environment. Adversaries may accomplish this by disabling individual services of high importance to an organization, such as MSExchangeIS, which will make Microsoft Exchange content inaccessible. In some cases, adversaries may stop or disable any or all services to render systems unusable. Services may not allow for modification of their data stores while running. Adversaries may stop services to induce data destruction or encrypt data for impact on the data stores of services like Exchange and Microsoft SQL Server.

Attackers can fake the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or call, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the CreateProcess API call, which supports a parameter that defines which PPID to use. This functionality is used by Windows features such as user account control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via svchost.exe or consent.exe) rather than the current user context.

Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of PowerShell or Rundll32 to be explorer.exe rather than an Office document delivered as part of spear phishing attachment. These spoofing techniques can be executed via Visual Basic for Applications (VBA) scripting within a malicious Microsoft

Office document or any code that can perform execution through an API.

Explicitly assigning the PPID may also enable privilege escalation, given appropriate access rights to the parent process. For example, an adversary in a privileged user space, such as an administrator, may spawn a new process and assign the parent as a process running as SYSTEM (such as lsass.exe), causing the new process to be elevated via the inherited access token.

Adversaries commonly use domain generation algorithms (DGAs) to procedurally generate domain names for command and control communication, and for other uses such as malicious application distribution. DGAs drastically increase the difficulty for defenders to block, track or take over the command and control channel, as there potentially can be thousands of domains that malware can check for instructions.

Threat actors can shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine. In some cases, these commands also may be used to initiate a shutdown/reboot of a remote computer. Shutting down or rebooting systems may disrupt access to computer resources for legitimate users. Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as a disk structure wipe, or inhibiting system recovery, to hasten the intended effects on system availability.

Attackers also interrupt the availability of system resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked or manipulated. Adversaries also may subsequently log off and/or reboot boxes to set malicious changes into place.

RECOMMENDATIONS

- ☑ Consider **implementing IT recovery plans** that contain procedures for consistently **testing data backups that can be used to restore critical data**. In some cases, the method to decrypt files affected by a ransomware campaign is released to the public
- ☑ **Research trusted sources** for public releases of decryptor tools or keys to reverse the effects of ransomware
- ☑ **Identify potentially malicious software** and audit and/or block it by using whitelisting tools

Hybrid Threat Actors

Hybrid threat actors present unique challenges because their classification is not always rigid. Common classes of hybrid threat actors include nation-states, cybercriminals, hacktivists and others described below. These actors may masquerade as a certain type to hide their true agendas. Or, threat actors may belong to two or more classes, switching between them as their priorities change.

NATION-STATES

Nation-state threat actors are often thought to possess resources and capabilities above and beyond the average threat actor. They have unique relationships to other types of threat actors, and they view cyber-threat actors within their boundaries according to philosophy and law. Citizens in a country are subject to the laws, regulations and governance of the nation-states in which they reside. Similarly, nation-state threat actors are not excluded from the laws and regulations of their own countries and therefore cannot act with impunity.

Analysts from Optiv and Digital Shadows weigh in below on prominent nation-states that engage in cyber-threat activity and use their positions to integrate domestic, non-nation-state threat actors into their offensive cyber policies.

» **China**. China prefers to indoctrinate cyber-threat actors so they willingly support the state. Feelings of patriotism and common achievement drive actors to cooperate and follow nation-state direction. China instills, and to an extent, enforces, a deep sense of loyalty to country through schooling and the military. Groups may be directly associated with the military (APT1/ Comment Crew), or they attract and maintain followers and members (Honker Union) via an agenda that focuses on patriotism and duty to country. China's recurring Five-Year Plan, which lays out key and strategic-level objectives related to economic growth, global influence, investments and culture, directs and influences the sentiment and actions of domestic cyber operations. China maintains a robust cyber capability within both its intelligence service, the Ministry of State Security (MSS) and the People's Liberation Army.

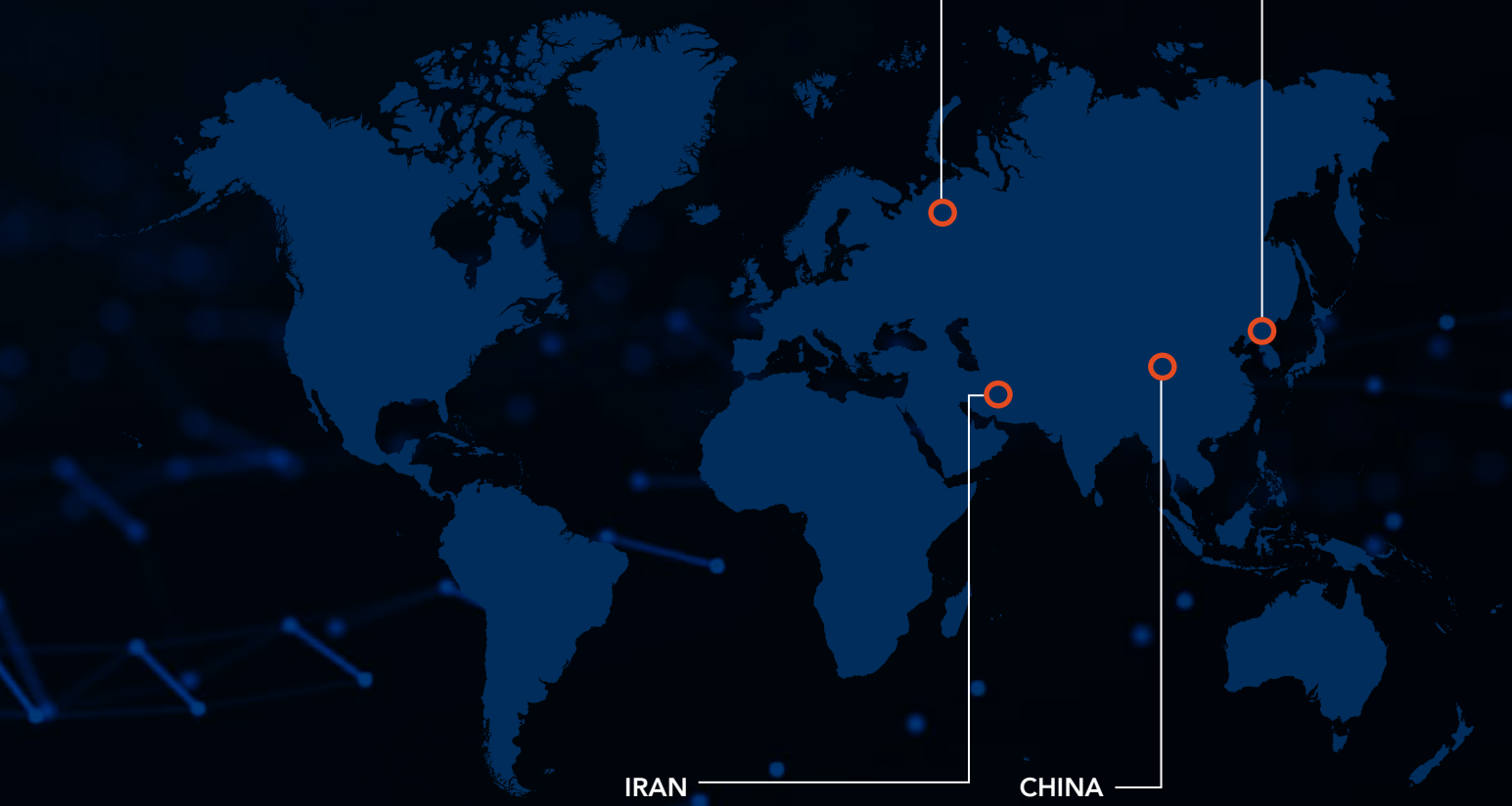
» **North Korea.** The North Korean government maintains a firm grip over its domestic cyber-threat actors. Its efforts are aided by the state's indoctrination methods so that technical skills are developed among those serving the government. When compared with other nation-states, North Korea's interests have had a greater focus on monetary gain brought on by the country's economic isolation and strict international sanctions imposed on the country. In addition to financially motivated activity, North Korea also engages in destructive cyber activity against South Korean media and targets other foreign media institutions that have portrayed the North Korean regime in a negative light. These actions were highlighted in cyber attacks carried out against international banks and cryptocurrency exchanges that were linked to the North Korean state. North Korea has been linked to the infamous WannaCry attack in 2017. The Lazarus Group/HIDDEN COBRA, an advanced persistent threat group, has been linked to several high-profile cyber attacks including the 2014 Sony Motion Pictures breach as well as attacks against South Korean critical infrastructure and media/financial institutions.

  Digital Shadows analysts found that the Lazarus Group was particularly active in 2019 – and well known for conducting operations for financial gain to raise government revenue. This is unusual for nation-state groups, which typically are focused on espionage operations used to gather sensitive political and military information. The majority of Lazarus Group's attacks on cryptocurrency exchanges took place in Asia – South Korea in particular.

2019 STATE OF NATION THREAT ACTORS

RUSSIA
allows cybercriminals to conduct their activities as long as they target entities outside of Russia's borders and accept cyber direction from state sources.

NORTH KOREA
have had a greater focus on monetary gain brought on by the country's economic isolation and strict international sanctions imposed on the country.



IRAN
actively cultivates and recruits non-nation-state actors.

CHINA
maintains a robust cyber capability within both its intelligence service, the Ministry of State Security (MSS) and the People's Liberation Army.

Cryptocurrency-related organizations remained a popular target for Lazarus. In addition to targeting multiple established cryptocurrency exchanges, the group also was linked to an operation that promoted a fake cryptocurrency trading program and installed a backdoor on a victim's device when downloaded. Lazarus also conducted more traditional espionage operations. For example, the group was linked to an operation targeting one of India's nuclear power plants, Kudankulam Nuclear Power Plant (KNPP), in October 2019. The Dtrack trojan used in the attack was developed by the group.

Although Windows remains the target operating system of choice for most threat actors, a notable trend was Lazarus' targeting of Mac OSX systems. South Korean OSX users were targeted through macro-embedded documents that would go on to execute a malicious PowerShell script. Lazarus often targeted both Windows and OSX users through the separation of infection procedures as part of the same operation.

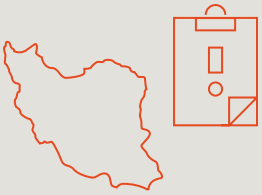
» **Iran.** Iranian nation-state actors actively cultivate and recruit non-nation-state actors in addition to continually building out their paramilitary cyber units such as APT33 and OilRig. Many Iranian threat actors carry out their activities by self-driven initiative as well as by suspected guidance from Iranian government and military organizations. Hacktivist groups, whose members sometimes have loose ties to higher education and military institutions, often are driven by the hope and expectation of being rewarded or recruited by special units within Iran's military and paramilitary groups that are involved in information security and cyber activity. The Basij, a volunteer corps, recruits for various domestic and national-level security initiatives, including cyber operations.

Reporting suggests that by late 2018, Iranian government officials took a stricter stance on its independent actors to reel in offensive cyber operations under tighter government control and guidance. Throughout 2019, there was a notable increase in aggressive Iranian activity that further degraded relations between Iran and the West. Iranian state-linked hacker groups continued to remain focused on conducting disruptive cyber attacks and spreading disinformation and pro-Iranian propaganda.[12] It's uncertain what the long-term response from Iranian groups will be in light of the strike that killed Islamic Revolutionary Guard Corps (IRGC) commander General Qasem Soleimani in January 2020.

According to Digital Shadows research, MuddyWater, an Iranian state-associated threat actor, was most active in the first half of 2019. But throughout the year, the group used many new or previously unobserved tools to conduct espionage operations targeting various sectors and regions, including the Middle East, Asia, Europe and North America. One campaign used a previously unseen PowerShell-based backdoor called POWERSTATS v3 to target a university in Jordan and a government entity in Turkey. The multi-staged backdoor exfiltrated information and staged a second-stage attack by obtaining additional payloads from MuddyWater's command and control (C2) server. MuddyWater also expanded its targets to include Android devices. Mobile malware deployed by the group enabled it to gather information – including contact lists, call logs, SMS text messages and Android geolocation information – from an infected device.

In the second half of 2019, there was a notable reduction in public reporting on MuddyWater, although it is possible that campaigns occurred in the second half of the year but were not reported. Similar to reporting of APT34 activity, a Telegram user leaked information on the threat actor in May 2019, including images of both MuddyWater C2 server source code and the back end of the C2 servers. Given the sophistication of the group, it is unlikely that this would have severely disrupted their operations. It is more likely that the lack of reporting was caused by reporting biases. Cyber-espionage campaigns often are reported either in retrospect or not reported until many months or years after they take place.

» **Russia.** The Russian state controls and coordinates cyber-threat activity with its non-nation-state actors via coercion. Cybercriminals are allowed to conduct their activities as long as they target entities outside of Russia's borders and accept cyber direction from state sources. Failure to do so can result in criminal prosecution. Russia is suspected of repurposing domestic hackers and threat actors that are embroiled in legal issues stemming from past cyber activities. These actors may be leveraged by government security and/or intelligence bureaus to carry out activities that benefit the state's agenda.



MuddyWater

In 2019, the Iranian state-associated threat actor MuddyWater targeted government and telecommunication organizations in the countries surrounding Iran. Phishing emails sent to targets contained Word documents that, once opened, displayed an error message to prompt a target into downloading a file. If a user proceeded, the malicious file established a connection with a C2 server that had links to previous MuddyWater attacks. The file exploited CVE-2017-0199 (a vulnerability previously exploited by the Iranian state-associated threat actor APT34) and ran a PowerShell script. The script obtained and exfiltrated information about the compromised system to the MuddyWater C2 server. The group also deployed additional, although unspecified, payloads onto compromised systems.

Because CVE-2017-0199 was used previously by APT34, it is possible that the two threat actors are collaborating with Iranian state-associated groups known to share infrastructure. Telecommunication organizations are an attractive target for espionage operations because they are part of a country's critical infrastructure and form critical nodes in a country's network. By gaining access to telecommunication organizations, a threat actor increases its ability to intercept and collect network traffic within a target country.

ACTORS WITH CRIMINAL INTENT

Cybercriminals are individuals or groups that typically conduct malicious attacks on networks for the purpose of stealing personally identifiable information (PII) or company data and making a profit from the theft. Two groups, TA505 and FIN6, were highly active in recent months.

» **TA505.** Both Optiv and Digital Shadows followed TA505 (also called Evil Corps), a financially motivated threat actor. TA505 has been active since 2014. Russia is its suspected home. Sophisticated TTPs have caused analysts to classify this group as an advanced persistent threat. This actor has a history of targeting banks, financial institutions and retailers across multiple countries including the United States. TA505 has likely expanded its operational capabilities as demonstrated by its attacks on new sectors and geographies. Attacks spanned targets in Asia, North America, South America and Africa. The breadth of organizations targeted by the group and the regularity of its operations indicate that TA505 can conduct multiple campaigns simultaneously.

  No TA505 activity can be construed as politically motivated, and no activity shows preference in its targets based on nationality. **One reason for the wave of cybercrime from within the former Soviet Union is a high level of technology talent combined with high unemployment.** Poor economic conditions create an environment in which technically skilled hackers and other offensive operators turn to criminal activity to generate income. In some cases, individuals may be members of more than one cybercriminal group. This is the case with indicted TA505 member Maksim Yakubets, who authorities have alleged was part of the criminal group running the GameOver Zeus botnet.[13]

  The majority of TA505 operations involved targeting victims with trojans used to gather and exfiltrate sensitive information. The group frequently used new or updated malware including ServHelper and Get2, and it was attributed to high-profile spam campaigns that distributed malware families such as Dridex, Locky and FlawedAmmyy.[14] The group's activity is believed to have caused more than $100 million in losses by the end of 2019 according to the United States Treasury Department.[15] During this period, two members of the group were indicted by United States authorities. One of these individuals was employed by the Russian government's Federal Security Service.

» **Fin6.** Digital Shadows reported on this sophisticated, financially motivated threat actor that **is well known for deploying malware on point-of-sale systems** in the retail and hospitality sectors. The group has moved beyond its traditional tactics to begin targeting e-commerce websites. The majority of Fin6 attacks directly targeted e-commerce websites, rather than securing access through a supply chain (such as compromising third-party payment platforms used on online checkout pages). Attacks against e-commerce organizations were likely intended to conduct card skimming. Payment details entered by customers at checkout are obtained and exfiltrated to a threat actor's command and control server.

  Fin6 also was linked to an operation targeting an unnamed engineering organization with the LockerGoga ransomware variant -- another attack vector not previously associated with the threat actor. Fin6 reportedly used stolen credentials to move laterally within the target network before attempting to deploy the ransomware, although the intrusion was contained, preventing the ransomware from infecting the system.

The reason behind Fin6's varying attack methods is unknown. One possibility is that Fin6 has changed its tactics as more profitable opportunities arose. The group continues to target point-of-sale (POS) systems, indicating its traditional attack vector remains popular. The group's operational sophistication likely means it can conduct different types of attacks.

» **ShinyHunters.** This threat group has been observed by Digital Shadows to be engaging in the sale of datasets obtained from organizations within a variety of sectors, including education, media and technology. **The group is known to sell allegedly stolen datasets on dark web criminal marketplaces**, notably Empire Market and RaidForums. The posts are labeled "first stage," indicating there may be a second stage posted in the near future. ShinyHunters initially gained prominence when the group listed 91 million Tokopedia user records for sale on Empire Market. Since then, it has added user records from additional organizations, including Ulmon, Zoosk, Bhinneka, Chronicle of Education, Home Chef, Minted, StyleShare, Ggumim, Mindful, Star Tribune and Chatbooks.

On May 6, 2020, ShinyHunters contacted security researchers to claim responsibility for stealing 500 GB of data from Microsoft's private GitHub repositories – this was posted on RaidForums by user "fsoc131ty." Fsoc131y maintained the same contact information within its forum bio as ShinyHunters, indicating that the user is likely associated with the ShinyHunter threat group.

ShinyHunters has been flagged for scamming users on RaidForums. The report states that the group did not deliver a database after a user paid for the data. On a separate dark web community, Dread, ShinyHunters responded to accusatory posts that implicated the threat group for refusing to refund 1.5 BTC for a database that was ordered by mistake. The posts also implicated ShinyHunters for compromising the user's account and carrying out a fraudulent transaction to buy a ShinyHunters database. The user requested that ShinyHunters refund the money for the transaction, as the user claimed not to have made the purchase and not to want the data. At the time of writing, ShinyHunters is refusing to refund the user's money.

ShinyHunters' activity is reminiscent of another threat collective, Gnosticplayers, which operated in a nearly identical fashion. ShinyHunters has listed millions of users' records for sale on criminal marketplaces and has repeatedly reached out to media sources to take responsibility for the breaches. Gnosticplayers is believed to be the group behind more than 40 breaches of large companies in 2019, and it contacted media outlets to claim responsibility. It is possible that ShinyHunters has connections to or is derived from members of the Gnosticplayers threat group.

Twitter account Shiny Hunters (@sh_corp) has been attributed to the ShinyHunters threat group. The profile was created in January 2020 and at the time of writing, maintains two tweets that reference news articles related to the Tokopedia breach. The Twitter profile also maintains a shiny Pokémon profile picture, indicating that the ShinyHunters name is potentially derived from Pokémon games. Within the game, Shiny Pokémon exist and players spend hours hunting for them. This clue may lend credence to the threat group's motivation: hunting for shiny or rare artefacts, which appear to be user data.

HACKTIVISTS

Hacktivism presents a threat to many industries and entities. Any organization can run afoul of a given hacktivist's ideological system. Ideological motivations can be economic, political, societal or environmental. Hacktivists provide tempting collaborators for nation-state actors in two ways. First, there may be overlaps in beliefs systems such that the hacktivist — intentionally or otherwise — conducts attacks on common targets. Second, these beliefs may be subverted via influence operations to create a cut-out organization that allows a nation-state actor to conduct attacks with plausible deniability.

Optiv analysts identified the following attack techniques that characterize hacktivists campaigns:

- **Defacements**, which allow attackers to get their message out in a prominent way with the least amount of skill necessary
- **DDoS attacks**, which require a relatively low level of skill while creating a publicly notable impact
- **Name-and-shame attacks**, which hacktivists use to infiltrate a system, exfiltrate potentially embarrassing material and leak it publicly. These attacks require greater skills, resources and coordination than DDoS and defacement attacks

COMMERCIAL ENTITIES

Optiv's gTIC studied commercial entities, which provide nation-states with a marketplace to enhance their offensive hacking and surveillance capabilities. Several commercial entities made the news in the past year, and they participate in the tangled international trade in cyber capabilities.

Through commercial entities, governments can acquire advanced cyber capabilities without having to train personnel to develop tools in-house. They also can maintain a leaner cyber operation with fewer personnel without sacrificing efficiency or capability. Because commercial entities are profit-based organizations, they aren't always restricted to serving other entities from a certain region or government. This flexibility allows them to provide services to organizations of their choice regardless of political or ethical differences with the government of the country in which the private organizations are based.

Data Breaches

Data breaches can be linked to a variety of causes: malicious activity, neglect, mistakes, and lack of awareness or visibility. The rate of data breaches continued its upward march in 2019. In healthcare, more data breaches were reported in April 2019 than in any other month to date – and a monthly average of 37.2 breaches occurred from January 2019 to May 2019, compared to a monthly average of 29.5 in 2018.[16] Other studies revealed that data breaches soared by 17% in 2019 compared to 2018,[17] and that 86% of breaches were financially motivated.[18]

Optiv experts weighed in below on privacy regulations, identity and data management, and Zero Trust – topics essential to a discussion about breaches.

WORLDWIDE PRIVACY REGULATIONS

Many companies in recent months wrapped up delayed efforts to implement the General Data Protection Regulation (GDPR) and weighed differences between GDPR and the California Consumer Protection Act (CCPA) as they considered future investment decisions. While emphasis on regulations, data privacy and data protection increased, overall adoption remained slow. One survey reported that privacy notices are, on average, over a year old and that the majority of companies have not updated their privacy notices for the CCPA.[19]

Privacy-related breaches in the news called attention to regulations, audits and enforcement. As a result, data inventories – which capture where data is processed, stored and transmitted – gained traction and were viewed as a necessary first step in implementing privacy regulations. Some companies, however, chose a tactical approach unconnected to a data governance program that can manage data shifts with automation. As a result, inventories go out of date.

Regulatory Momentum

Countries and states, and even industries, develop their own regulations and/or data privacy laws. According to a United Nations report, 107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy. While the status of legislation is evolving, the breakdown as of the writing of this report was:

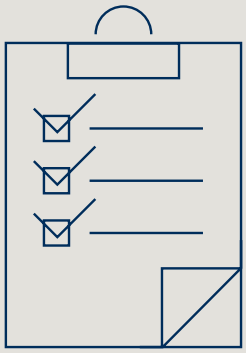
66%
of countries with legislation

10%
of countries with draft legislation

19%
of countries with no legislation

5%
of countries with no data[20]

States in the United States are in varying stages of developing privacy laws, although there are 16 provisions that commonly appear in statutes.[21] Some of these are:



California Consumer Protection Act

Privacy rights regulations such as the CCPA give consumers the right to understand how their personally identifiable information (PII) is used, to opt in or opt out, and to request that their data be deleted (the right to be forgotten). Compliance depends on PII being identifiable and manageable across all data and security controls, regardless of where the PII is located – on premises, in the cloud or in third-party systems. To request changes in how their PII is handled, consumers fill out data subject access requests (DSARs).

Noncompliance can result in substantial fines. The CCPA provides for recovery of up to $750 per consumer per incident or actual damages, whichever is greater, along with other types of relief.[22]

- The right of consumers to access personal information collected or shared
- The right of consumers to correct personal information, request deletion of personal information and to restrict a business' ability to process personal information
- The right to opt out of the sale of personal information
- Notice/transparency requirements
- Data breach notification

RECOMMENDATIONS

- ☑ **Implement company-wide data governance**, including third parties, to ensure that all data is inventoried and can be managed throughout its lifecycle
- ☑ **Build a privacy management program** that accommodates most applicable regulations, leaving only a small number for special handling
- ☑ **Apply controls that are common** across regulatory environments to minimize duplication and wasted effort
- ☑ **Rely on threat intelligence and analysis** to understand who is interested in which data and why – and implement proper protections
- ☑ **Use automation and orchestration** to eliminate data silos, expedite compliance and improve enterprise-wide reporting

IDENTITY AND DATA MANAGEMENT

Traditional identity access management (IAM) programs continue to evolve in response to fluid organizational perimeters, digital transformation, user access practices, use of personal devices and massive data growth. According to IBM research, 90% of the world's data existing today did not exist two years ago.[23] Forecasts for data growth are sobering. In 2025, 49% of the world's stored data will reside in public cloud environments, up from only around 20-25% in 2018.[24] The lack of appropriate access controls is a leading risk factor, yet over 70% of organizations admit they have users who have more access privilege than required for their job.[25]

Fortunately, the historic silos of identity management and data governance began to merge into identity and data management (IDM) programs. Business leaders recognize that silos increase risk and complicate efforts to eliminate vulnerabilities, comply with privacy rights and deliver a positive user experience. Improvements in these areas depend on visibility into who is accessing systems and how they are doing it. Visibility expands when identity and data are brought together in a common data management framework.

Authentication Uptick

The forces mentioned above that are bringing identity and data together have triggered changes in authentication methods. Passwords, which are still ubiquitous, are increasingly viewed as security liabilities. They are targeted in part because organizations no longer have stable network perimeters, and even complex passwords now can be decrypted rather easily. And, while inexpensive to set up, passwords are expensive for IT to support. Alternative forms of authentication are both established and nascent, and those connected to customer experience or revenue generation are the most likely to be prioritized and funded.

Multifactor authentication (MFA), which has been around for a long time, remained underutilized. Native support for MFA is common, but the next advance is likely to be integration with digital identity proofing tools.

Passwordless authentication has become a more frequent discussion topic. It verifies identity based on something that is unique to a user, such as a biometric signature, hardware token or a piece of information. Passwordless use has not been more widely adopted due to regulatory uncertainties.

Managing Elevated Credentials

Research showed that approximately 70% of internal data breaches are caused by privilege abuse[26]—internal actors misuse their level of granted access. Further, 53% of companies have 1,000+ sensitive files accessible to every employee.[27] For this reason, privileged access management (PAM) remained a critical solution. It is strongly recommended for DevOps, DevSecOps, financial operations and groups working with intellectual property. Some companies applied PAM to third-party remote access, and more needs to be done in this area.

PAM supports the processes and technical controls related to accounts with elevated permissions and access to critical assets. Typically, it functions to:

- Discover privileged accounts.
- Locate and classify data.
- Apply user analytics.
- Manage passwords.
- Monitor and track privileged access activities.
- Block unauthorized access.

There are many ways to design PAM solutions, but all should include basics such as managing credentials through vaulting and rotation, limiting executable commands and setting frequent reauthentication requirements.

RECOMMENDATIONS

- ☑ Follow **Zero Trust principles**
- ☑ Implement PAM to better **safeguard critical assets**
- ☑ Enforce **micro-segmentation** and the **least-privilege** model
- ☑ Use **artificial intelligence**, **machine learning** and **user behavior analytics** to simplify authentication and enhance usability

Establishing Secure Network Access

A business process outsourcing company implemented MFA for its workforce, with requirements for minimal disruption, strong data access controls and identity integrity. Steps taken:

- Participated in a workshop to better understand the networks, assets and applications to be secured for business continuity – included Microsoft Office 365, cloud-hosted resources and servers using MFA for Microsoft Windows and SSH
- Established remote VPN, which connected with an MFA solution
- Streamlined registration using risk-based access policies

2019 IDM USE CASES AND TRENDS

GETTING STARTED WITH PAM

A global medical device organization developed a comprehensive PAM program by taking the following actions:

- Developed a long-term strategy to address current and future privileged account risks
- Established a worldwide infrastructure to support multiple locations
- Migrated data from old to current version levels
- Took a multi-phased approach to secure privileged accounts on high-risk business systems and infrastructure

> **Over 60% of new data** created in 2023 will require some level of protection, but **only half will be protected**.[29]

PASSWORDS: USERS' BAD HABITS PERSIST, INCREASING RISK

In companies with more than 1,000 employees, the average employee was expected to have about 25 unique logins.[28] Despite the risks associated with passwords, many employees still do not adhere to cybersecurity best practices – and in some cases, bad habits not only persist but are getting worse. SailPoint identified several trends:

75%
of respondents reuse passwords across different accounts. This is a practice that is becoming more frequent over time – in 2014, only 56% admitted to reusing passwords.

23%
change their work passwords two or fewer times per year. This is considerably better than for personal accounts, however, where over two-thirds (67%) of respondents change their password as infrequently.

47%
of respondents duplicate passwords across work and personal accounts.

15%
of respondents would consider selling their workplace passwords to a third party.

Zero Trust

Zero Trust has gained greater visibility with cybersecurity leaders, causing this security approach to be a more sought-after solution. Industry analyst firms presented their frameworks, and cybersecurity vendors focused on how they implement Zero Trust based on their technology/expertise niches. The many definitions and perspectives, however, contributed to confusion and inertia.

Zero Trust has been talked about for years. It bubbled up to the top of security discussions due to common business pain points:

» Legacy perimeter-based security strategies do not address all security risks

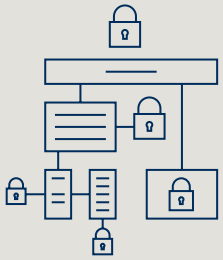
» Cloud adoption exposes vulnerabilities and security complexities

» Enormous data growth poses a challenge for classifying and controlling data

» Users expect a unified experience regardless of which devices they are using and how and where they access data

Viewed through the right lens, Zero Trust is quite straightforward and not as daunting as it may seem. Why? Because most companies already have Zero Trust-compatible components in place. Rip-and-replace is not required or advisable. The greatest Zero Trust activity in recent months occurred in three areas: privileged access management, multi-factor authentication and software-defined perimeter.

> By 2023, the **average CIO will be responsible** for more than **three times the endpoints** they managed in 2018.[30]



Zero Trust in a Nutshell

Zero Trust helps you manage risk by reducing the exposure of vulnerable systems and preventing the lateral movement of malware throughout your network. There is no single Zero Trust solution. Zero Trust works best based on a custom plan that puts identity and data at the center. And keep in mind that *identity* refers to whatever/whoever performs an action in the environment – user, computer, IoT device, mobile phone, etc.

A Zero Trust model operates by not trusting any entity on the network – users, devices or applications. By establishing "trust nothing and no one" boundaries, you can compartmentalize segments of your network. Segmentation allows greater control over who has access to critical assets, limits user access, increases control over applications and scans for potential threats as users access allowed resources.

A PRACTICAL PATH TO ZERO TRUST

A useful way to think about Zero Trust is that technology is important, but the greater success factor relates to how Zero Trust components are put together. A basic roadmap involves three stages:

» **Fundamental.** Progress toward Zero Trust involves asking what's been done, what can be used and what's next. Components such as network access controls, an identity directory and firewalls can be repurposed. Typical focus areas include authentication/authorization, user role definition, data protection and network security.

> One study revealed that **92% of respondents** plan to **adopt a multi-cloud strategy**.[31]

» **Integrated.** Companies break away from standalone security components and connect silos with solutions that combine data and identity. Examples include privileged access management, dynamic governance and software-defined perimeters. A mature security information and event management (SIEM) system operates in a security orchestration, automation and response (SOAR) environment.

» **Adaptive.** Authentication is risk-based. Access isn't always granted immediately, but it is evaluated immediately. Artificial intelligence and machine learning support governance-on-demand. Networks, identities and policies are fully integrated and enforced.

RECOMMENDATIONS

☑ **Find a knowledgeable partner to** help you along the journey; The Zero Trust "final destination" is an evolving threshold at which you can manage risk based on your objectives

☑ **Begin at the beginning with Zero Trust fundamentals** and do them well; If this layer isn't based on sound principles, it may need to be redone

☑ **Pursue policy-based data governance** – classifying, labeling, defining information – with the "who and why" of identity in mind

☑ **Establish analytics.** Track events inside various technology solutions; Tie events to identity and data so you know if orphaned events are taking place without an identity context; Choose key performance indicators (KPIs) that align with business objectives

NOTABLE BREACHES

Digital Shadows contributed a list of high-profile incidents and data breaches involving third parties. Third-party risk involves organizations losing data after a supplier was compromised and through the exposure of their own data through unsecured external cloud servers. Notable breaches include:

BANKING

A large, United States-based bank announced the theft of personally identifiable information (PII) in July 2019 of American and Canadian nationals who had either applied for, or possessed, credit card products. The data was stolen by an individual named Paige Thompson, who used compromised credentials to gain initial access to an Amazon Web Services (AWS) bucket used by the bank. Thompson previously worked for Amazon as an engineer (although not at the time of the breach) and was reportedly able to gain access to the bank's data by exploiting a misconfigured firewall on a web application.

IT SERVICES

India's third largest IT outsourcing company experienced an intrusion into its network in April 2019. The breach provided the threat actor behind the operation with substantial access to both the company's networks and clients. The incident was initially thought to be conducted for espionage purposes, although it was later reported that the attackers were interested in obtaining email credentials to access portals managing gift card and rewards programs.

> More than **21 million accounts** for employees of Fortune 500 companies **were found available for sale on the dark web**

SOFTWARE

A threat actor gained intermittent access to a United States-based software company's network between October 2018 to March 2019. Security researchers linked the attack to a cyber espionage campaign by the Iranian state-associated threat group Iridium. An estimated 6 to 10 terabytes of data were stolen. The breach was particularly significant given that the software company handled sensitive projects for the White House communications agency, the United States military, the FBI and multinational companies.

FORTUNE 500

More than 21 million accounts for employees of Fortune 500 companies were found available for sale on the dark web. Despite the high number of compromised accounts, the methods used to gain login credentials were unsophisticated. Researchers determined that approximately 95% of the credentials contained unencrypted or brute-force cracked, plaintext passwords. The majority of collected passwords were weak and easy to guess.

APT34

Threat actors experienced data breaches after a user named Lab Dookhtegan published information on the victims, the data that was gathered and the tools used by the Iranian state-associated group APT34. Lab Dookhtegan also doxed Iranian Ministry Intelligence officers by posting PII.

Dark Web

The number of dark web listings that could harm an enterprise has risen by 20% since 2016.[32] According to Digital Shadows analysts, stolen data typically lands on a dark web marketplace, where cybercriminals buy and sell it for nefarious purposes. Some marketplaces accept custom orders for PII, which allows bad actors to steal identities.

A proactive enterprise cybersecurity team keeps an eye on for-sale information, the types of assets offered and their value – all clues to current and potential future targets. Dark web intelligence shows who is interested in which data, helping you implement proper protection.

DARK WEB MARKETPLACES

Goods for sale include passports and documents, carding guides, accounts, counterfeit money, malware, databases and gift cards.

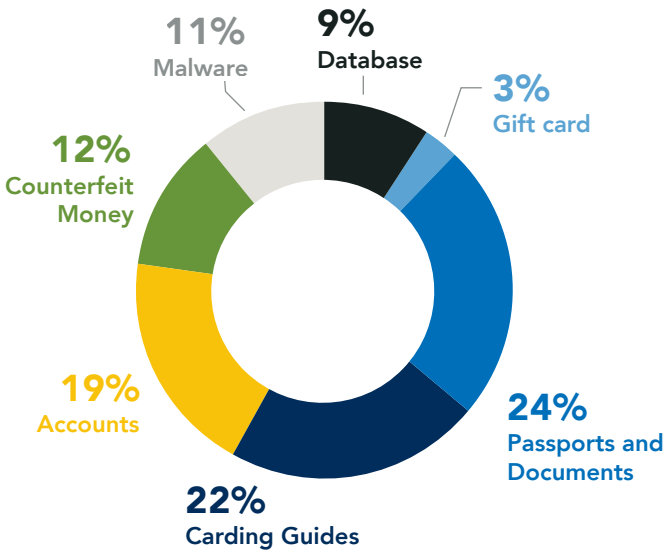


Figure 8 - Goods for sale on the dark web in 2019 (Digital Shadows).

DARK WEB BY THE NUMBERS

Based on the number of listings, the top dark web marketplaces were Nightmare, Berlusconi, Empire, Apollon, Wall Street and Tochka.

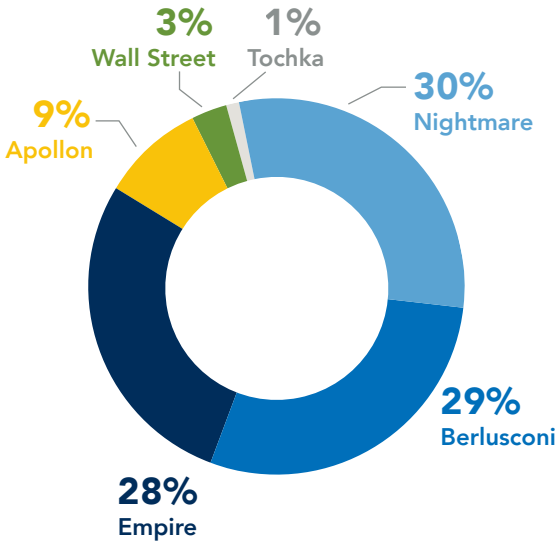


Figure 9. Top dark web marketplaces in 2019 (Digital Shadows).

RECOMMENDATIONS

- ☑ **Use in-house or external tools** to monitor the cybercriminal landscape for threats to your organization and third-party vendors
- ☑ **Monitor for employee credentials included in leaked databases;** On notification, change credentials and protect accounts with multi-factor authentication; Do not reuse passwords across multiple services; Consider using a reputable password manager to store and generate secure, unique passwords; Deactivate valid accounts for former employees upon departure
- ☑ **Audit and document all software used by your organization;** This can reduce the pain of patch management; Critical security patches should be applied as soon as they are made available; Do not rely on legacy or end-of-life software
- ☑ **Limit your organization's attack surface** by ensuring only devices critical for business operations are connected to the internet; Network storage devices, databases and other internet-facing services should be appropriately secured; Practice the principle of least access by restricting administrative access and elevated privileges only to employees who require these credentials

Conclusions

Threat intelligence provides essential insights into security breaches, the impact they have on enterprise data and the disposition of stolen data. Business leaders and security practitioners can strengthen risk management policies and cybersecurity programs by understanding threat actors, attack tools, attack techniques, data breaches and the dark web.

Both the threat landscape and cybersecurity countermeasures are dynamic, requiring constant oversight and timely action. Many organizations engage a service provider to augment their threat analysis efforts and help implement a proactive defense based on best practices:

- ☑ **Implement company-wide, policy-based data governance**, including affiliated third parties, to ensure that all data is inventoried and can be managed throughout its lifecycle
- ☑ **Audit internal, external and third-party assets** regularly to determine if they are current, in compliance, misconfigured or no longer needed
- ☑ **Build a privacy management program** designed to accommodate most applicable regulations so only a small number require special handling
- ☑ Maintain rigorous identity and data management controls by **adopting a Zero Trust model**, enforcing micro-segmentation and adhering to the principle of least privilege
- ☑ **Implement a privileged access management program** to protect your most critical assets
- ☑ **Use multi-factor authentication** wherever possible and especially with third-party services, databases and APIs
- ☑ **Conduct regular security awareness training** to educate employees about risks, teach them how to report suspicious activity and explain what they can do to avoid risky behaviors
- ☑ **Establish meaningful analytics based on KPIs** aligned with your business objectives

CONTRIBUTORS

Thank you to threat intelligence analysts and cybersecurity experts at Optiv, VMware Carbon Black, Digital Shadows, Palo Alto Networks and SailPoint who contributed to this report.

REFERENCES

1. The Hill, Hackers Find New Target as Americans Work from Home During Outbreak. March 14, 2020.
2. Optiv blog, How Can You Determine the Risk of a Threat Actor? March 5, 2019.
3. VMware Carbon Black, 2019 Holiday Threat Report. December 2019.
4. Deloitte, Cybersecurity for Smart Factories. 2020.
5. Verizon, 2019 Data Breach Investigations Report. 2019.
6. E&E News, Experts Assess Damage After First Cyberattack on U.S. Grid. May 6, 2019.
7. Gartner press release, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020." August 29, 2019.
8. ZDNet, US Coast Guard Discloses Ryuk Ransomware Infection at Maritime Facility. December 30, 2019.
9. Reuters, Ransomware Attack at Mexico's Pemex Halts Work, Threatens to Cripple Computers. November 11, 2019.
10. Wired, Decades-Old Code Is Putting Millions of Critical Devices at Risk. October 1, 2019.
11. New Jersey Cybersecurity and Communications Integration Cell, Threat Profile. December 15, 2016.
12. Defense One, Suspected Iranian Cyber Attacks Show No Sign of Slowing. July 3, 2019.
13. Naked Security, $5m Bounty Set on the Alleged Head of Evil Corp Banking Trojan Group. December 9, 2019.
14. Trend Micro, TA505 At It Again: Variety is the Spice of ServHelper and FlawedAmmy. August 27, 2019.
15. Department of Treasury, Treasury Sanctions Evil Corp, the Russia-based Cybercriminal Group Behind Dridex Malware. December 5, 2019.
16. HIPAA Journal, May 2019 Healthcare Data Breach Report. June 20, 2019.
17. Identity Theft Resource Center, 2019 Data Breaches. January, 2020.
18. Verizon, 2020 Data Breach Investigations Report. 2020.
19. Zetoony, David, Survey of Fortune 500 Companies' Privacy Representations. Bryan Cave Leighton Paisner LLP. December 2019.
20. United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide.
21. IAPP Resources, US State Comprehensive-Privacy Law Comparison.
22. International Association of Privacy Professionals, Resource Center, California Consumer Privacy Act of 2018.
23. IBM Marketing Cloud, 10 Key Marketing Trends for 2017.
24. IDC, Data Age 2025: The Digitization of the World. November 2018.
25. Cybersecurity Insiders, IAM Survey. August 2019.
26. Verizon, Data Breach Investigations Report, 2019.
27. Varonis, Global Data Risk Report. 2019.
28. LastPass, 2019 Password Security Report. October 2019.
29. IDC, Security and the Global DataSphere: A Data-Driven World Needs Its Data Protected, June 2019.
30. Gartner, Top Strategic IoT Trends and Technologies Through 2023. September 2018.
31. RightScale, State of the Cloud Report. 2019.
32. McGuire, Dr. Michael, Back Into the Web of Profit: Going Undercover in the Dark Net, Uncovering Threats to the Enterprise. May 30, 2019.

Want to learn more?

Visit www.optiv.com/intelops

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | www.optiv.com

Secure your security.™

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.