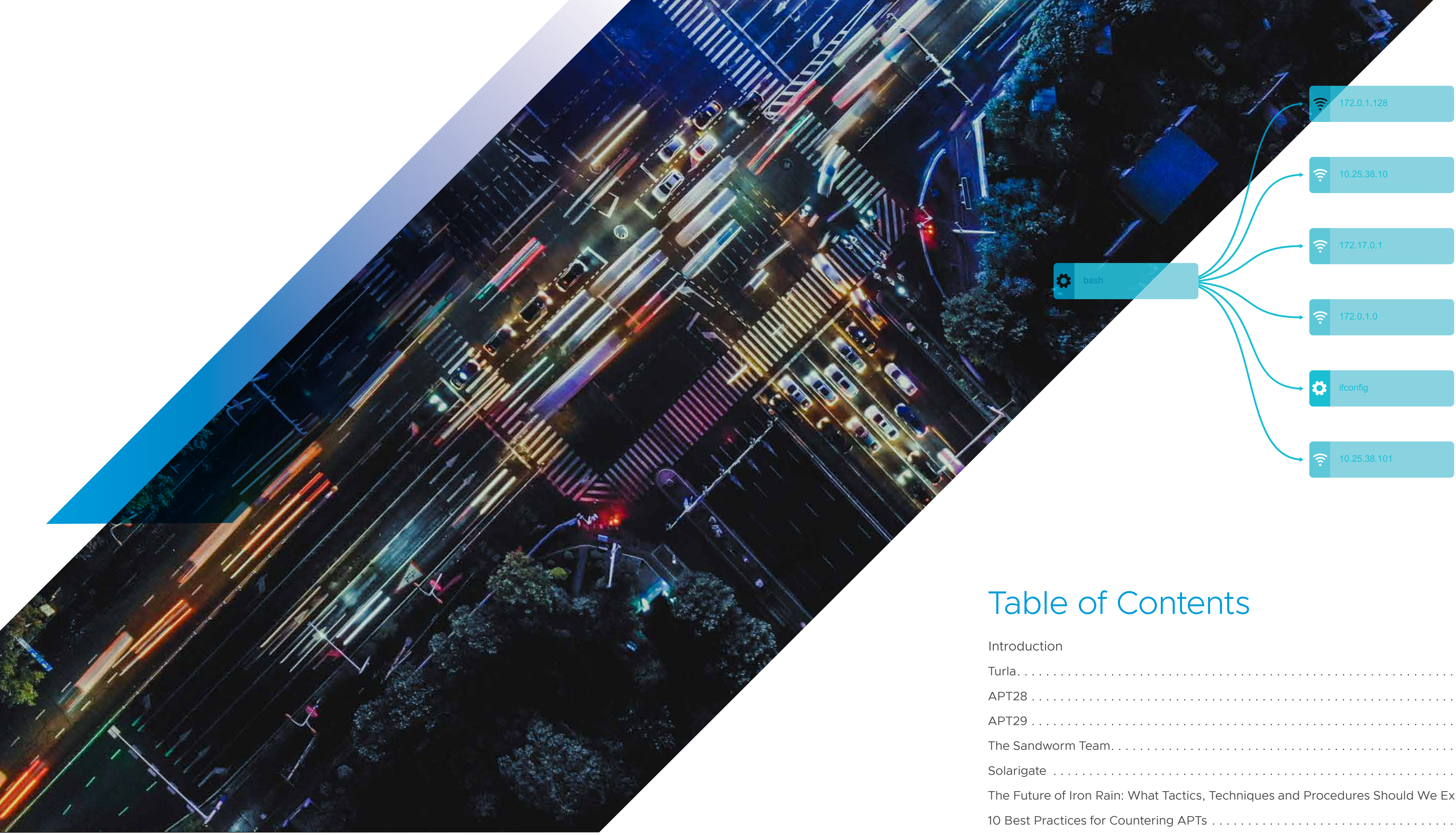
Iron Rain: Understanding Nation-State Motives and APT Groups

February 2021



> "I ran from the wolf but ran into a bear."
> — Russian Proverb

Tom Kellermann, Head of Cybersecurity Strategy, VMware
Greg Foss, Senior Cybersecurity Strategist, VMware

Table of Contents

Introduction 3
Turla. 5
APT28 7
APT29 8
The Sandworm Team. 9
Solarigate 11
The Future of Iron Rain: What Tactics, Techniques and Procedures Should We Expect? . .14
10 Best Practices for Countering APTs 15
Sources 17
About VMware 18

Introduction

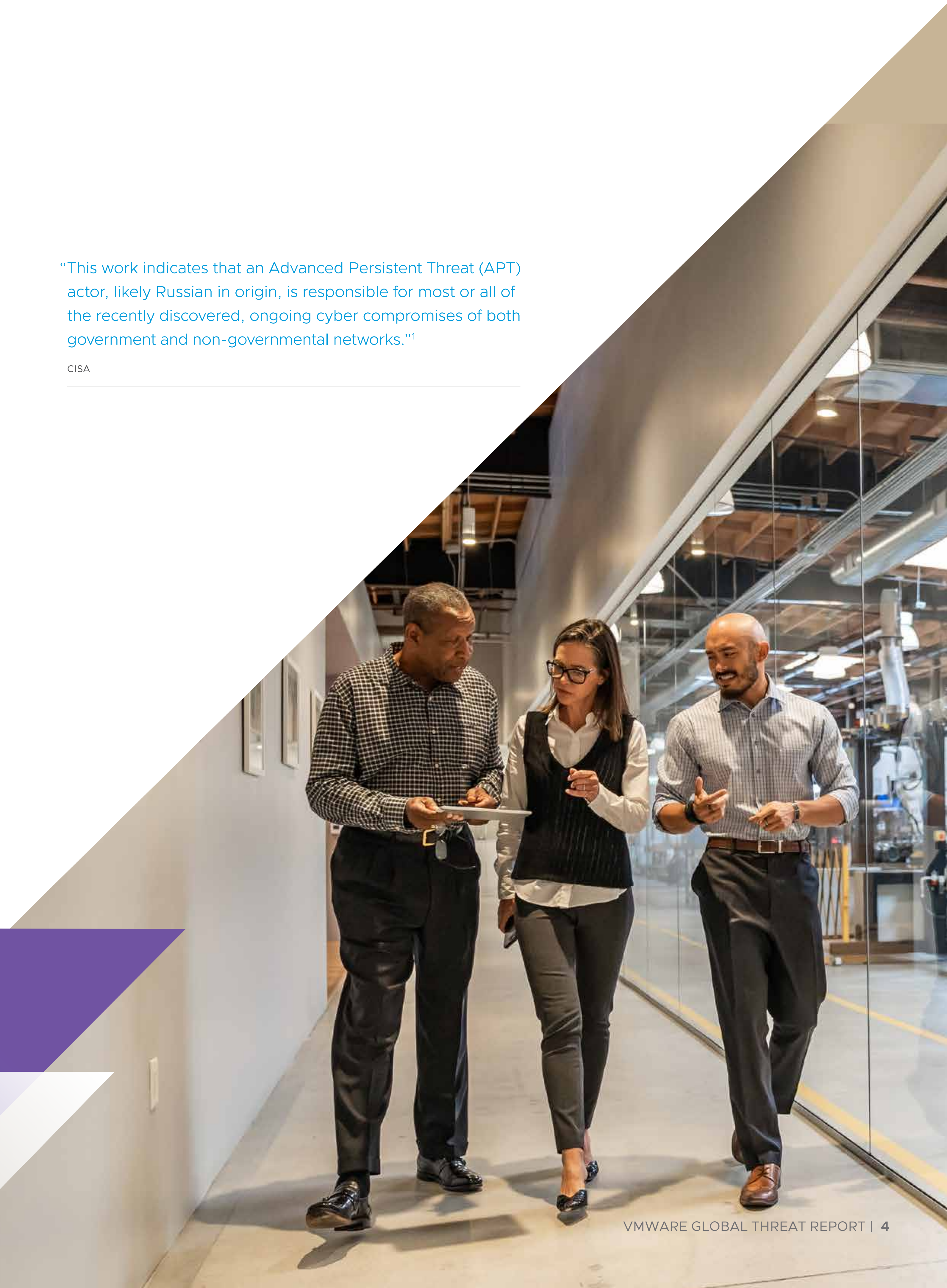
Last December, the security industry was stunned by the magnitude and sophistication of the SolarWinds breach. Today, efforts are still underway to assess the impact of the more than seven-month-old cyberespionage campaign. In January, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigations (FBI), the Office of the Director National Intelligence (ODNI), and the National Security Agency (NSA) issued a joint statement announcing the plan to coordinate the investigation and remediation of the SolarWinds attack, which they cited as a significant cyber incident involving federal government networks.[1] While the agencies work to understand the scope of the incident, the current investigative and mitigation efforts conclude:

"This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly."

In 2013, the Russian chief of the General Staff gave an infamous speech outlining an operational concept to confront the west with hybrid warfare. The Gerasimov doctrine is a whole-of-government concept that fuses hard and soft power across many domains and transcends boundaries between peace and wartime.[2] The doctrine is an effort to develop an operational stratagem for Russia's confrontation with the west. A stratagem founded in the principle that the Achilles heel of the U.S. is its dependency on technology, a dependency that can be undermined and corrupted via cyberespionage. Four primary APT groups serve as the vanguard—Turla, APT28, APT29 and the Sandworm Team—along with various others that are suspected to be involved with cyberespionage on behalf of the Russian government. The threat actors who have risen to prominence following the SolarWinds compromise are also believed to be highly skilled Russian cyber operatives.

This report will explore the tactics, techniques and procedures (TTPs) of these groups over the years as well as predictions on the subsequent evolution of their operations in 2021 and beyond. It brings together research and analysis from the VMware *Howlers*, the *VMware Threat Analysis Unit™*, and the security industry.

> "This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks."[1]
>
> CISA



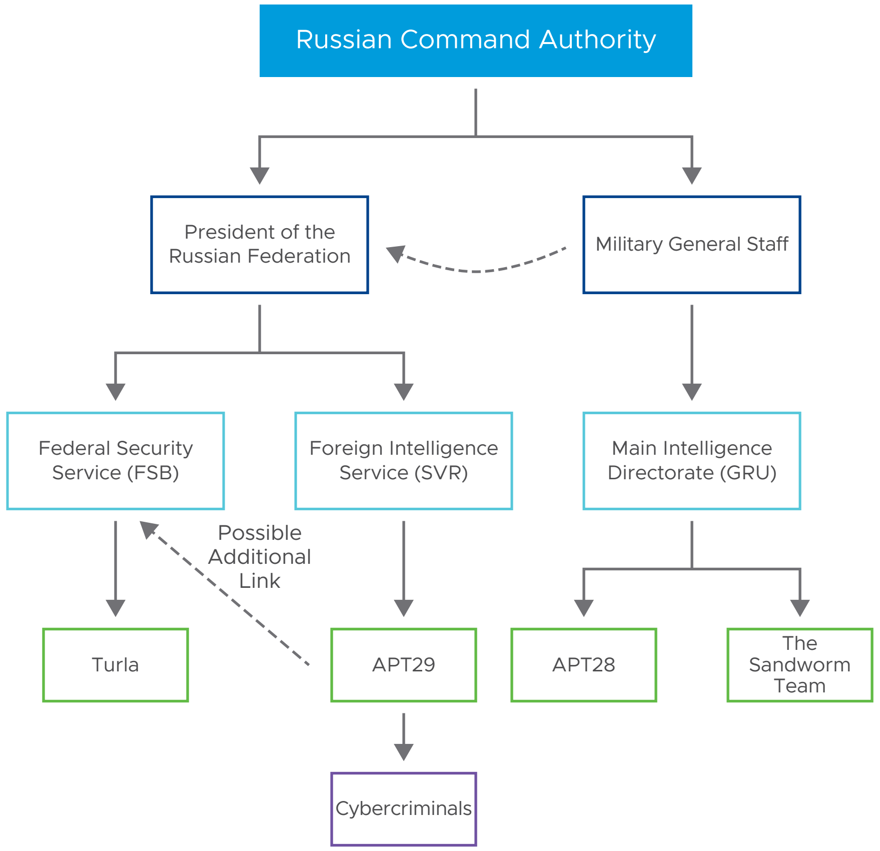

Russian Command Authority
President of the Russian Federation
Military General Staff
Federal Security Service (FSB)
Foreign Intelligence Service (SVR)
Main Intelligence Directorate (GRU)
Possible Additional Link
Turla
APT29
APT28
The Sandworm Team
Cybercriminals

FIGURE 1: Russian cyber military hierarchy.[3]

Turla

Turla[4] is the oldest of the high-end nation-state backed threat actors. The group became world renowned for leveraging the Moonlight Maze campaign.[5] In the mid-1990s, Turla launched the first major cyberespionage campaign. The campaign was hallmarked by low and slow attacks to steal U.S. military secrets through a backdoor. The group successfully breached vast amounts of classified information. This was the first time defense officials feared Turla may have maintained access to later sabotage their systems.

Through the years, researchers have observed that Turla continues to advance their methods and operations—most prominently, the clandestine techniques that were leveraged to exfiltrate sensitive data and operationalize compromised infrastructure.[6] Turla demonstrates a deep understanding of technology and human psychology, resulting in a level of sophistication seldom paralleled across the cybercrime spectrum. While they are most well known for targeting Windows systems, they have also demonstrated unique tradecraft for Linux and macOS.[7] Specifically, VMware uncovered unique usage of the group's PNG Dropper, which has been leveraged extensively to evade endpoint detections across their victims.[8]

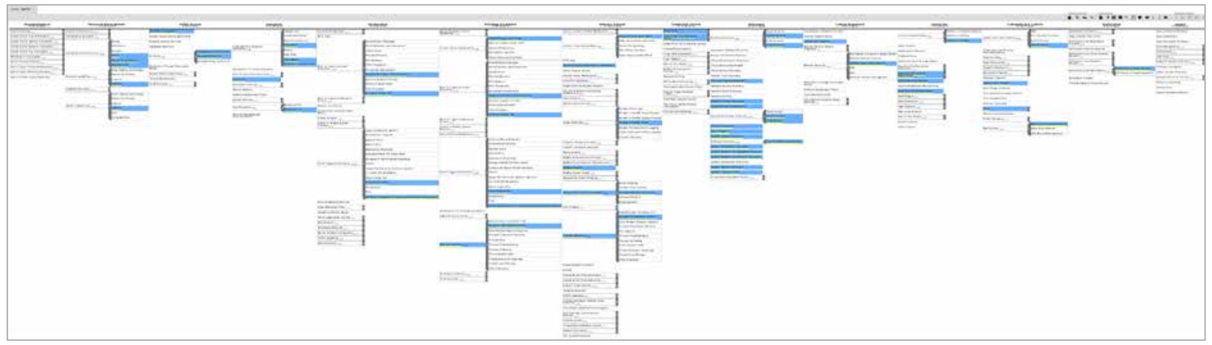


FIGURE 2: Active MITRE ATT&CK Navigator layers for Turla.

VMware has observed that Turla's preferred method of initial access is via spear phishing and establishing watering holes through the compromise of soft targets, utilizing primarily web-based payloads such as Java and Adobe binaries delivered in the form of software updates. These deception techniques continue once inside the target organization's networks, often prompting victims to install fake Microsoft applications. Turla is known to use common publicly available tooling, such as Mimikatz, for credential access and has more recently been observed using Metasploit for lateral movement.

Turla has also been known for zero-day attacks targeting the Microsoft Office suite of software to leverage for initial access and privilege escalation over the years. The group is known for handling the initial exploitation and access governance for their targets. Typically, post-exploitation and lateral movement have been handled by different teams that leverage their own unique tradecraft through the remainder of the operation.

Turla

Zoom in on the active MITRE ATT&CK Navigator layers.

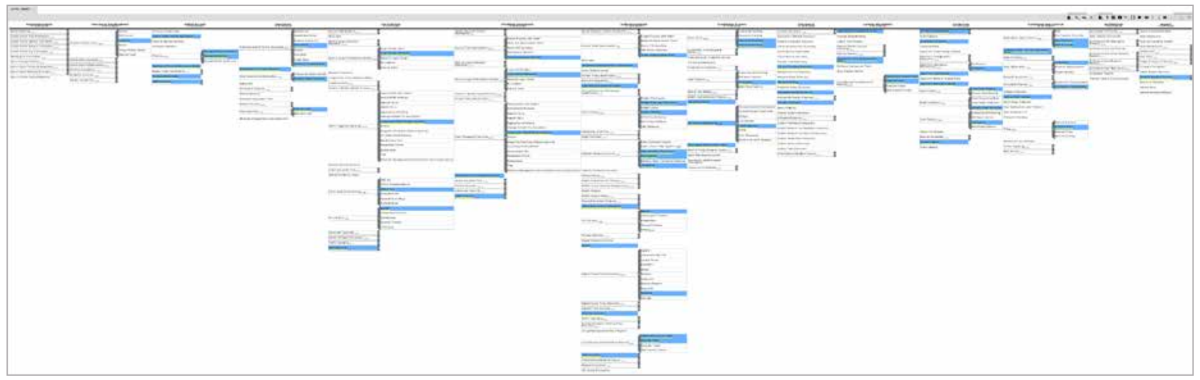


FIGURE 3: Active MITRE ATT&CK Navigator layers for APT28.

APT28

The APT28[9] threat group has been active since 2004 and publicly attributed to the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165.[10] The group gained worldwide notoriety for their involvement in interfering with the 2016 U.S. presidential election, specifically the large-scale compromise of the Hillary Clinton campaign, the Democratic National Committee (DNC), and the Democratic Congressional Campaign Committee in 2016.[11] Members of APT28 were indicted by the United States in 2018 along with additional GRU cyber operators.[12]

Drovorub is the Linux malware that acts as an implant and includes a kernel module rootkit. This malware can handle bidirectional file transfer and act as an intermediary command and control server. This is a unique piece of malware in the APT28 bag of tricks that primarily targets Windows systems using living-off-the-land techniques with the goal of targeting sensitive communications, namely emails, and exfiltrating this data in a clandestine fashion.

APT28

Zoom in on the active MITRE ATT&CK Navigator layers.

APT29

APT29[13], otherwise known as the Dukes of Moscow or Cozy Bear, is a Russian government threat group that has been a known entity since 2008. It's believed the group operates either under the Russian Foreign Intelligence Service (SVR) or the Russian Federal Security Service (FSB).[14] They primarily target government ministries, government agencies, political think tanks, and often government subcontractors. The group is primarily focused on espionage and gained international prominence for their alleged involvement in compromising the DNC servers in summer 2015.[15]

APT29 leverages a wide array of custom-tailored malware in their operations, and primarily relies on phishing as their initial means of entry. VMware has observed the group taking full advantage of PowerShell as part of their post-exploitation toolkit as well, which not only provides ample means for them to extend their attack capability, it also provides great visibility for endpoint detection and response. So much so that VMware developed a PowerShell module to simulate this activity in a safe and controlled manner.[16]

The group has been inactive from 2017–2019, though they appear to have reemerged with updates to known tooling during Operation Ghost, which targeted the Ministries of Foreign Affairs in at least three different countries across Europe.[17] Throughout all of their operations, they leverage a common string routine, where the strings are encoded as a sequence of hexadecimal digits, with every two hexadecimal digits decoding into a single character. This routine has been observed by VMware researchers and MITRE in their tradecraft dating back to 2013, with a majority of their recent operations leveraging Cobalt Strike extensively for post-exploitation and lateral movement.

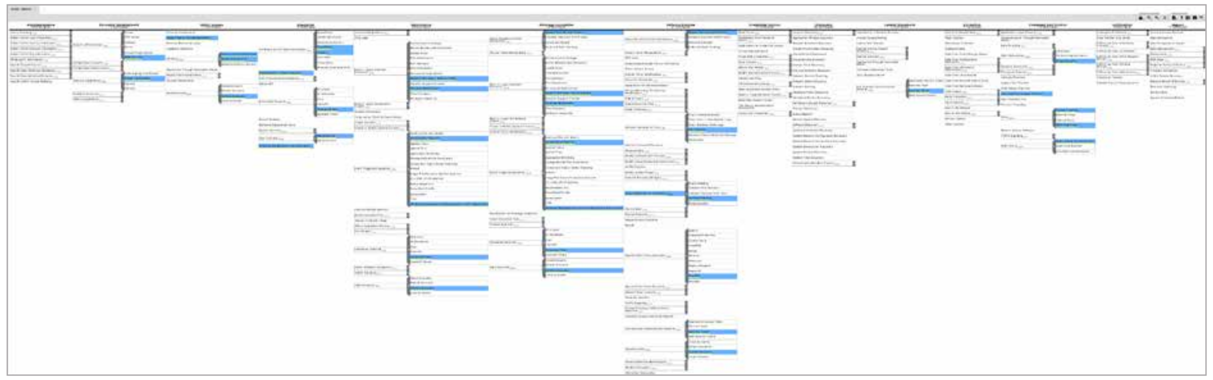


FIGURE 4: Active MITRE ATT&CK Navigator layers for APT29.

APT29

Zoom in on the active MITRE ATT&CK Navigator layers.

The Sandworm Team

The Sandworm Team[18] is known for destruction. The group has been active since 2009 and was attributed to Russian GRU Unit 74455 by the United States Department of Justice. The Sandworm Team is believed to be behind some of the most devastating cyberattacks with kinetic impact the world has ever seen.[19]

Crash Override, a devastating modular piece of malware, was most famously leveraged in the Ukraine power grid cyberattack of December 2016, which left hundreds of thousands of citizens without power.[20] This was just the beginning of this group's wave of cyberattacks.

NotPetya, manufactured by the Sandworm Team, was based on the original Petya ransomware, though lacked the ability for victims to recover their data by randomly generating the unique system identifier, VMware researchers found. This new variant was also equipped with the SMB spreading capabilities of EternalBlue and EternalRomance, two NSA hacking tools that were stolen during the infamous Shadowbrokers leak.[21] Perhaps most interesting is the fact that NotPetya was deployed via a backdoor in the popular Ukraine accounting software, M.E.Doc. The resulting impact of this breach was catastrophic to many companies and has been estimated to have cost $10 billion in damages globally.[22]

The Sandworm Team is a formidable adversary, capable of large-scale PsyOps and espionage, largely focusing on cascading and tangible impact across their targets. VMware researchers have found that the Sandworm Team has even shown a willingness to attack Russian-owned companies to establish plausible deniability. The Sandworm Team's actions over the years have not gone unnoticed, with members of the group being indicted on computer fraud and conspiracy charges by the United States Department of Justice in October 2020.[23]

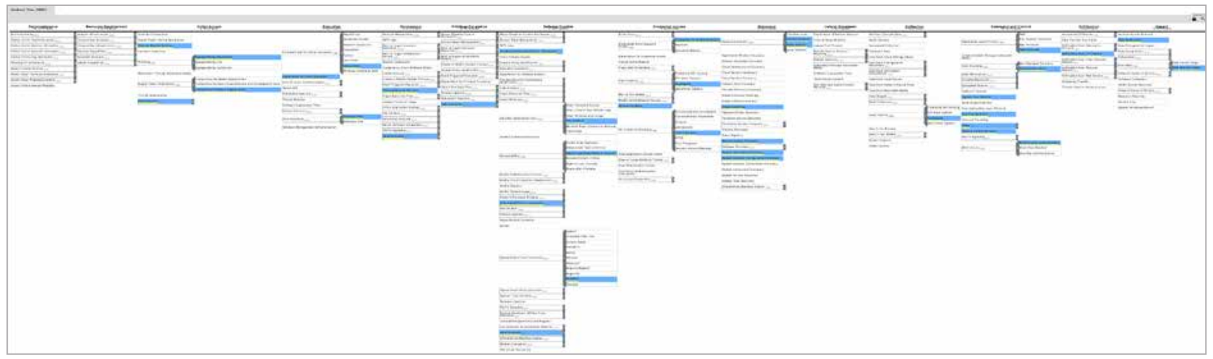


FIGURE 5: Active MITRE ATT&CK Navigator layers for the Sandworm Team.

The Sandworm Team

Zoom in on the active MITRE ATT&CK Navigator layers.

Solarigate

As 2020 prepared to come to an end, the security industry learned of one more impactful event—a cyberespionage operation that had been underway for the better part of the year. SolarWinds, a global leader in IT operations software, was compromised. The SolarWinds software was backdoored through a complex, intricate, and well-executed supply chain attack.[24] Leveraging the SolarWinds software update process allowed the adversaries to deliver the backdoor, labeled as Sunburst, to more than 18,000 organizations across the globe.

While the group responsible for this breach has not yet been definitively attributed, CISA has stated the attack is likely Russian in origin.[1] The organizations impacted include some of the largest and most influential companies and government agencies in the United States. However, the attackers were able to go undetected for a significant amount of time.

Further investigation of the malware highlighted the incredibly sophisticated defense evasion and persistence techniques within the backdoor. In addition to a 12- to 14-day sleep timer, anti-analysis techniques, and a modular and staged approach to infection, a majority of post-exploitation activity was done manually. Combined with the credentials obtainable via the SolarWinds Orion platform, the adversary was able to blend in with regular network activity, a process vastly simplified due to the expected behavior of Orion.

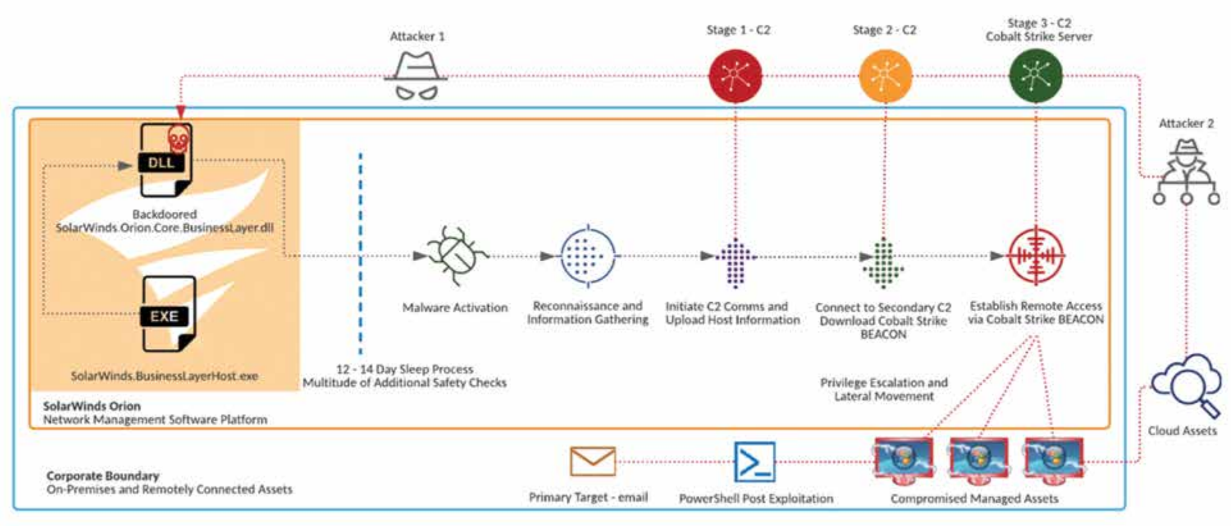

Attacker 1
Stage 1 - C2
Stage 2 - C2
Stage 3 - C2
Cobalt Strike Server
Attacker 2
DLL
Backdoored
SolarWinds.Orion.Core.BusinessLayer.dll
EXE
SolarWinds.BusinessLayerHost.exe
SolarWinds Orion
Network Management Software Platform
12 - 14 Day Sleep Process
Multitude of Additional Safety Checks
Malware Activation
Reconnaissance and Information Gathering
Initiate C2 Comms and Upload Host Information
Connect to Secondary C2 Download Cobalt Strike BEACON
Establish Remote Access via Cobalt Strike BEACON
Privilege Escalation and Lateral Movement
Cloud Assets
Corporate Boundary
On-Premises and Remotely Connected Assets
Primary Target - email
PowerShell Post Exploitation
Compromised Managed Assets

FIGURE 6: Sunburst backdoor command and control.

Solarigate

Zoom in on the active MITRE ATT&CK Navigator layers.

Researchers have also uncovered substantial code overlap between Sunburst and a well-known .NET backdoor that was previously written by Turla, known as Kazuar.[25] Specifically, this is the sleep algorithm and extensive usage of the FNV-1a hash for victim identification and related components of the backdoor.

The combinations of these findings and related threat groups highlights the unique interweaving of Russian nation-state threat actors, their ingenuity, and ever-evolving technical aptitude. Most importantly, it solidifies their place as one of the longest-running and impactful nation-state espionage groups.

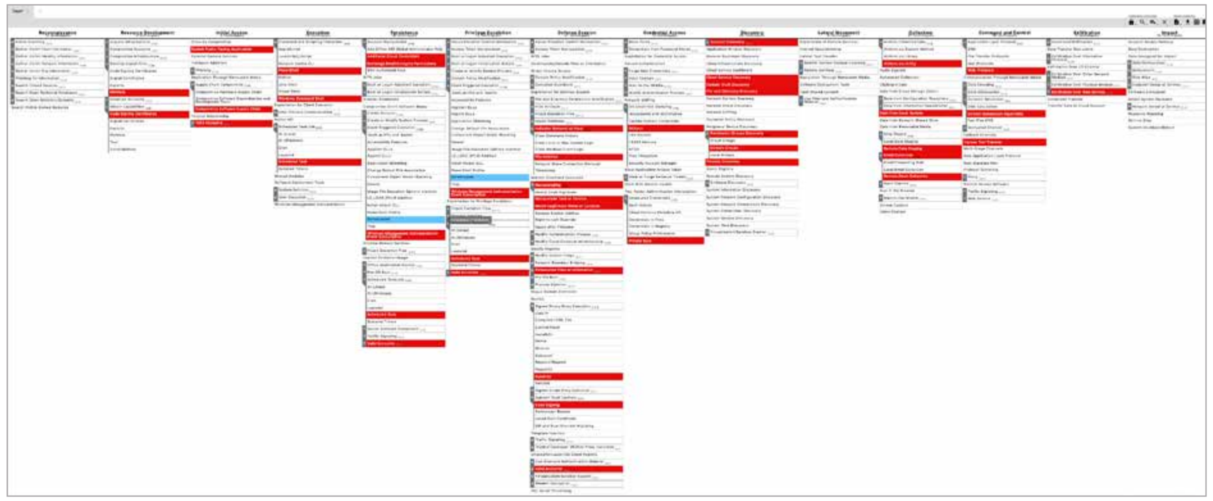


FIGURE 7: Active MITRE ATT&CK Navigator layers for Solarigate.

Solarigate

Zoom in on the active MITRE ATT&CK Navigator layers.

On February 3, 2021, NIST issued best practices for countering these adversaries.

Read the article.

The Future of Iron Rain: What Tactics, Techniques and Procedures Should We Expect?

Going forward, we anticipate that these threat actors will escalate their attacks against the west, following ongoing testing and validation of tactics across Ukraine.[26] A new administration also changes the threat landscape as we consider support of the North Atlantic Treaty Organization (NATO). As the U.S. and its allies attempt to contain the threat posed by the regime, cyberattacks and the use of proxies may grow. This reality forces all organizations—private and public sectors—to take a forward-leaning approach to cybersecurity. Organizations should look to subscribe to Zero Trust architectures that extend across their infrastructure intrinsically to suppress these threat actors.

"As cybercriminals continue to evolve and develop increasingly sophisticated methods of attack, law enforcement is likewise sharpening our investigative approaches necessary to arrest and convict these criminals," said David Smith, special agent in charge of the Criminal Division, U.S. Secret Service. "While criminal methods may change as technology advances, we must never forget that no matter how sophisticated criminals may become, they are human, and humans make mistakes. Law enforcement will always be there to exploit those mistakes."

"After the fall of the Soviet Union, Russian intelligence officers pivoted quickly toward the future of espionage," said Eric O'Neill, national security strategist, VMware. "The new generation of Russian spy prepared for a second cold war fought in cyberspace by observing the way that the internet created new pathways to information. In the late '80s, Russian spies spent a year compromising U.S. military and government networks across the United States in an operation named Moonlight Maze. They launched attacks from middle-man computer systems to mask their presence. In 2016, Russian spies leveraged this old playbook to compromise the United States election and weaponize stolen information. The recent SolarWinds attack demonstrates that Russian cyberespionage has taken that old '80s playbook to an elite level. The future of cybersecurity is not defending a perimeter but hunting the spies that find their way through."

11 Best Practices for Countering APTs

“Our mission from day one has been to help keep the world safe from cyberattacks,” said Patrick Morley, SVP and general manager, Security Business Unit, VMware. “We have been longtime advocates of cyber-hygiene principles that focus on protecting mission-critical business applications and data. These basic principles have never been more important and, when adhered to, can make a meaningful difference.”

1. Conduct behavior-based threat hunting:
   - Spend time reviewing the telemetry available, and get a baseline for normal behavior and events over time. The more effort you put in upfront toward understanding the environment and tuning events, the more dividends this will pay in the long run.
   - Understand the threats most commonly impacting your industry vertical, and focus on hunting for evidence of historical events using published indicators of compromise, threat intelligence feeds, and related information.
   - Test your security controls using open source frameworks to simulate adversarial behavior, such as Atomic Red Team by Red Canary, to ensure visibility and defense in depth.
2. Operationalize hardening and patching:
   - Leverage industry best practices for hardening and patching as they relate to your industry vertical.
   - Ensure IT operations and security are on the same page with vulnerability data and have agreed on service-level agreements (SLAs) for patching.
3. Implement multifactor authentication. Protect all external-facing assets with multifactor authentication.
4. Leverage a single sign-on (SSO) provider to allow for centralized and seamless authentication across the vastly distributed work environment.
5. Apply the principle of least privilege:
   - Role-based access is a key component to limiting access to sensitive data and preventing potential information leakage and exposure, accidental or otherwise.
   - Forcing an adversary to elevate privileges to move laterally, disable security tooling, and the like will force malicious actors to trip bells and whistles, and give the security operations center (SOC) more of an opportunity to detect and prevent the adversary from progressing.
6. Set up secure communication channels when responding to an incident. Today’s attackers will often attempt to monitor communications—especially those of the security team. The first and arguably most important step is to set up out-of-bands communication channels so you can discuss and share information without giving away that you are actively looking into their activities.
7. Assume the adversary has multiple avenues back into the organization. Resisting the urge to shut them out will pay dividends in the long run. Be patient, wait, watch, learn, and only strike when you are reasonably sure about the scope and breadth of the intrusion.
8. Baseline your organization to combat alert fatigue:
   - Overworked security teams are using detection tools more than ever, yet doing so can overwhelm these teams even more, while drowning out what’s important.
   - To combat this, an organization should map out where their most important assets lie, and then build out controls and tune security systems around those priorities. From there, security teams can begin a broader inventory management process, bucketing certain assets into logical groupings for more effective incident response (IR).
9. Build the capacity to detect and respond across workloads:
   - In the transition to a remote, cloud- and service-focused IT landscape, the security and management of workloads themselves becomes imperative.
   - Protect the cloud environments, containers and microservices where most of the work is happening today—the applications that exist between a system’s networks and its endpoints.
10. Apply micro-segmentation. Limit an adversary’s ability to move laterally within the organization. Forcing intruders to cross trust boundaries provides an improved opportunity for detection and prevention.
11. Segment personal and professional networks. Amid COVID-19, the corporate perimeter has expanded in employee homes, ushering in a deluge of new focus toward on-home routers and networks, which is only made more challenging with the lack of visibility security professionals have into those networks (especially while they, too, work from home).

While the stealthy network communication tactics and obfuscated binaries of APT groups make them hard to detect, all organizations—public and private—need to be constantly thinking about how they can stay one step ahead of attackers. VMware will continue to monitor their activity to provide insight and information to our customers. To learn more, please visit the *VMware Carbon Black website*.

Sources

This report may contain hyperlinks to non-VMware websites that are created and maintained by third parties who are solely responsible for the content on such websites.

1. Cybersecurity and Infrastructure Security Agency. "JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)." January 5, 2021.
2. VPK. "The value of science in foresight." February 26, 2013.
3. DomainTools. "The Devil's in the Details: SUNBURST Attribution". Joe Slowik. January 14, 2021.
4. MITRE ATT&CK. "Turla." October 22, 2020.
5. VICE. "New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group." Kim Zetter. April 3, 2017.
6. National Security Agency. "Turla Group Exploits Iranian APT To Expand Coverage Of Victims." October 21, 2019.
7. ESET Research. "Diplomats in Eastern Europe bitten by a Turla mosquito." January 2018.
8. VMware. "Partner Perspectives: Insight on Turla PNG Dropper." December 11, 2018.
9. MITRE ATT&CK. "APT28." October 6, 2020.
10. National Security Agency. "Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware." August 2020.
11. CrowdStrike. "CrowdStrike's work with the Democratic National Committee: Setting the record straight." June 5, 2020.
12. U.S. Department of Justice. "United States District Court Western District of Pennsylvania Indictment – United States vs. Aleksei Sergeyevich Morenets, et al." October 3, 2018.
13. MITRE ATT&CK. "APT29." October 22, 2020.
14. F-Secure. "The Dukes: 7 Years Of Russian Cyberespionage." September 2015.
15. Krebs on Security. "U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise." December 14, 2020.
16. VMware. "Invoke-APT29: Adversarial Threat Emulation." Greg Foss. January 29, 2020.
17. ESET Research. "Operation Ghost: The Dukes aren't back – they never left." October 17, 2019.
18. MITRE ATT&CK. "Sandworm Team." July 4, 2020.
19. U.S. Department of State. "The United States Condemns Russian Cyber Attack Against the Country of Georgia." February 20, 2020.
20. WIRED. "'Crash Override': The Malware That Took Down a Power Grid." Andy Greenberg. June 12, 2017.
21. CSO. "Petya ransomware and NotPetya malware: What you need to know now." Josh Fruhlinger. October 17, 2017.
22. WIRED. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Andy Greenberg. August 22, 2018.
23. WIRED. "US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit." Andy Greenberg. October 19, 2020.
24. FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor." December 13, 2020.
25. ThreatPost. "SolarWinds Hack Potentially Linked to Turla APT." Tara Seals. January 11, 2021.
26. CYBERWARCON. "The Secret Life of Sandworms." July 24, 2020.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit *vmware.com/company*.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com