Threats Unmasked

2021 Cyber Threat Intelligence Report

accenture

Foreword

Accenture Cyber Threat Intelligence (Accenture CTI) has been creating relevant, actionable threat intelligence for more than 20 years. But the rapid pace of cyber threat evolution means that intelligence needs to be timely to be relevant. As a result, we are changing our annual Cyber Threatscape report to a more frequent review, to help decision makers plan and act faster.

In this inaugural issue we highlight early 2021 cyber threat trends and expert perspectives on threats to the operational technology (OT) landscape. In an era of unprecedented uncertainty, with so many devices scattered throughout enterprise networks, it's challenging for security professionals to keep pace with security demands.

The SolarWinds and Colonial Pipeline incidents and the large-scale disruptions and cost of ransomware operations, illustrate the growing impact of cyber threat activity on enterprise risk across all industry segments. This risk is increasingly difficult to control and mitigate across both IT and OT environments.

While running industrial systems is eased by virtualization in the cloud and the advance of Internet-connected devices, these technologies are also introducing operational environments to new vulnerabilities and risks.

The global ransomware crisis has entered a new phase, as threat actors adopt stronger pressure tactics and new targets—in particular, manufacturing and critical infrastructure. Ransom impact is more widespread, with attacks often highlighting weaknesses in a company's security posture. Yet, despite Colonial Pipeline's recent admission of a US$4.4M payout,[1] victims cannot assume paying a ransom will restore data or prevent leaks[2] and it seems they recognize that—median ransom payments have fallen from US$110,532 in September 2020 to US$$78,398 in March 2021.[3]

As we have seen with the SolarWinds compromise, software supply chain security and third-party compromise vectors are in the spotlight. More generally, ransomware deployment is faster and more diverse, making pre-infection defense extremely difficult.

Enterprise risk management is a team sport that requires a variety of capabilities, a cohesive team, excellent execution of the basics and a willingness to adapt to changing conditions.

Security leaders must demonstrate to the C-suite and the board not only that they understand the criticality of the continuity of operations, but also the importance of working in partnership with the whole business to effectively manage risk.

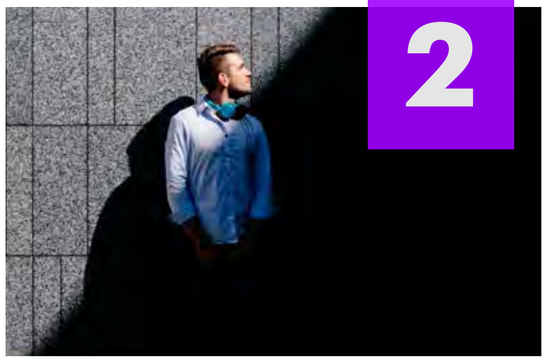
For more, take a look at our larger security library through our **Threat Intelligence**, **Cyber Defense**, and **OT Security** blogs and our recent **Operation: Next** OT security summit.

Howard Marshall
Managing Director, Accenture Security

Key trends

Following analysis in the first half of 2021, Accenture CTI identified four trends that are affecting the IT and OT landscape:

Ransomware actors test new extortion methods



Cobalt Strike is on the rise

Commodity malware can invade OT from IT space

Dark Web actors challenge IT and OT networks

Ransomware actors test new extortion methods

Ransomware actors are expanding data leak extortion, devising new methods to pressure victims.[4] Their creative approaches are hitting home as they place operational resilience—already tested by the disruptive forces of the pandemic—under increased pressure.

Threat actors are targeting new industries, using higher-pressure tactics to escalate infection consequences and deploying payloads faster to render trusted detection methods too slow. Response options are becoming more complicated.

Organizations should focus on preparation, prevention and pre-encryption defenses.

What's happening?

Targets are shifting

Small manufacturers remain typical targets,[5] but cases in the first months of 2021 targeted critical infrastructure—the May 2021 Colonial Pipeline ransomware paralyzed fuel distribution in much of the southeastern United States—and upstream providers, such as data-rich insurance companies.[6] Ransomware operators disrupt production in organizations that cannot afford downtime and feel pressure to pay ransoms. One group exploited a cloud provider's product to breach legal, transportation, geophysical and logistics entities.[7]

Tactics are toughening

Ransomware actors generally promise to decrypt their victims' systems and destroy stolen data after receiving ransoms,[8] but these promises are unreliable. Ransomware negotiator Coveware reported multiple cases in late 2020 where data was destroyed rather than just encrypted, preventing data retrieval even after ransom payment.[9] But, one group extorted their victims and posted stolen data without even deploying ransomware—apparently viewing exposure as more intimidating to its victim than "bricking" machines.[10]

Extortion is becoming personal
New exposure tactics, pioneered in 2020, have gathered speed, compounding data leak extortion damage, adding reputation damage to victim liability lists. In what one report has dubbed "quadruple extortion," groups are not only encrypting files and threatening to leak data, but also threatening non-payers with distributed denial-of-service (DDoS) attacks[11] [12] [13] or contacting victims' customers or business partners, urging them to pressure victims to pay ransoms.[14] [15] [16] [17] DarkSide, the group whose ransomware the FBI has said was responsible for the Colonial attack,[18] is one of the first to offer all four services as part of its affiliate service.[19] Clop actors focused on top executives' information, seeking blackmail material.[20] Babuk ransomware operators have joined Clop and Snatch actors in gaining broader exposure for their stolen victim data with anti-establishment activist communities.[21] After the fallout from the Colonial Pipeline hack led major underground forum administrators to ban talk of ransomware, Babuk announced a new platform where anyone can publish their stolen data.[22]

Tactics, Techniques, and Procedures (TTPs) are more advanced
Ransomware actors are developing new tools and exploits rapidly. Actors exploit new vulnerabilities—for example, alternative delivery mechanisms such as third-party hosting;[23] Accenture CTI identified notable defense evasion tactics with Hades ransomware operators using tooling and hands-on-keyboard actions to disable endpoint defenses.[24]

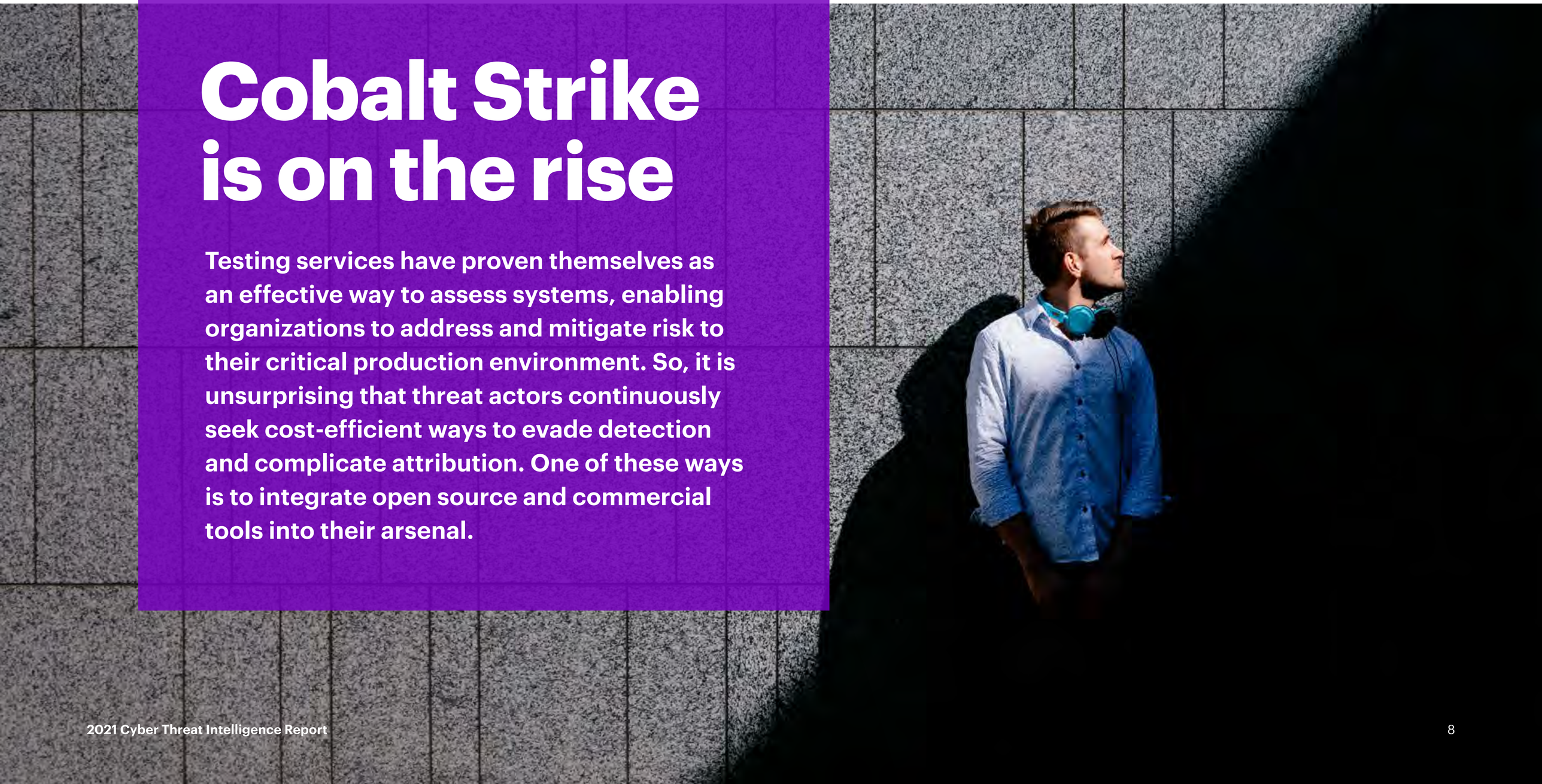
Where next?

To help tackle the impact of ransomware:

- **Nip attacks in the bud:** Organizations focusing on preparation, prevention, and pre-encryption defense can more effectively face the ransomware crisis.[25] [26] Segregation and zero-trust measures can limit threat actor movements if breaches occur.
- **Collaborate and report:** Collaborate with industry partners, consortiums and law enforcement for greater threat awareness.
- **Update risk and mitigation plans:** Apply an appropriate risk mitigation strategy that includes aspects such as controls deployment or secure data transmission mechanisms.

Cobalt Strike is on the rise

Testing services have proven themselves as an effective way to assess systems, enabling organizations to address and mitigate risk to their critical production environment. So, it is unsurprising that threat actors continuously seek cost-efficient ways to evade detection and complicate attribution. One of these ways is to integrate open source and commercial tools into their arsenal.



Since at least December 2020, Accenture CTI has observed, from internal research and public reporting,[27] a notable increase in threat actors adopting pirated versions of the commercial penetration testing framework Cobalt Strike.

This pirated software has enabled highly impactful campaigns, including the recently discovered SolarWinds-based compromises, as well as prolific "name-and-shame" ransomware attacks.

Accenture CTI invests significant resources in tooling that identifies, decrypts and tracks Cobalt Strike configurations in the wild.[28]

The framework's "Beacon" backdoor contains commercial watermarks, which enable analysts to monitor campaigns and target trends about locations of cracked or pirated Cobalt Strike deployments.

Public discussions around the prolific success of a malicious tool can often result in the development of new security detection techniques, leading threat actors to retool. However, due to numerous factors such as increased customization, the current high profile success of Cobalt Strike abuse means the pirated tool's popularity is actually growing—a trend that will almost certainly continue through 2021.

Organizations need to adopt new defensive tools that can counter this growing threat.

What's happening?

Cobalt Strike is proliferating

Although in use for more than a decade, the number of Cobalt Strike-enabled attacks reportedly increased by 163% between 2019 and 2020.[29] The emergence of pirated Cobalt Strike being abused as a preeminent commodity alternative to malware has occurred for numerous reasons.

In addition to being increasingly accessible, recent Cobalt Strike versions are more customizable than previous versions. As Accenture CTI observed in the recent SolarWinds breach,[30] threat actors are exploiting Cobalt Strike's malleable command-and-control features to customize default settings of the framework's Beacon backdoor and defeat detection.

Attack tools are evolving
Threat actors are evolving their own custom loaders to deliver Cobalt Strike. Notably, attackers developed several custom Cobalt Strike loaders to facilitate the SolarWinds campaign.[31] Accenture CTI has seen the popularity of the tool surge in the first three months of 2021.

Beyond the intensifying use of Cobalt Strike by opportunistic "name and shame" ransomware groups such as REvil (also known as Sodinokibi) and Egregor, Hades ransomware operators have also abused the tool to deploy their ransomware.[32] These ransomware attacks affected multiple victims between December 2020 and March 2021.

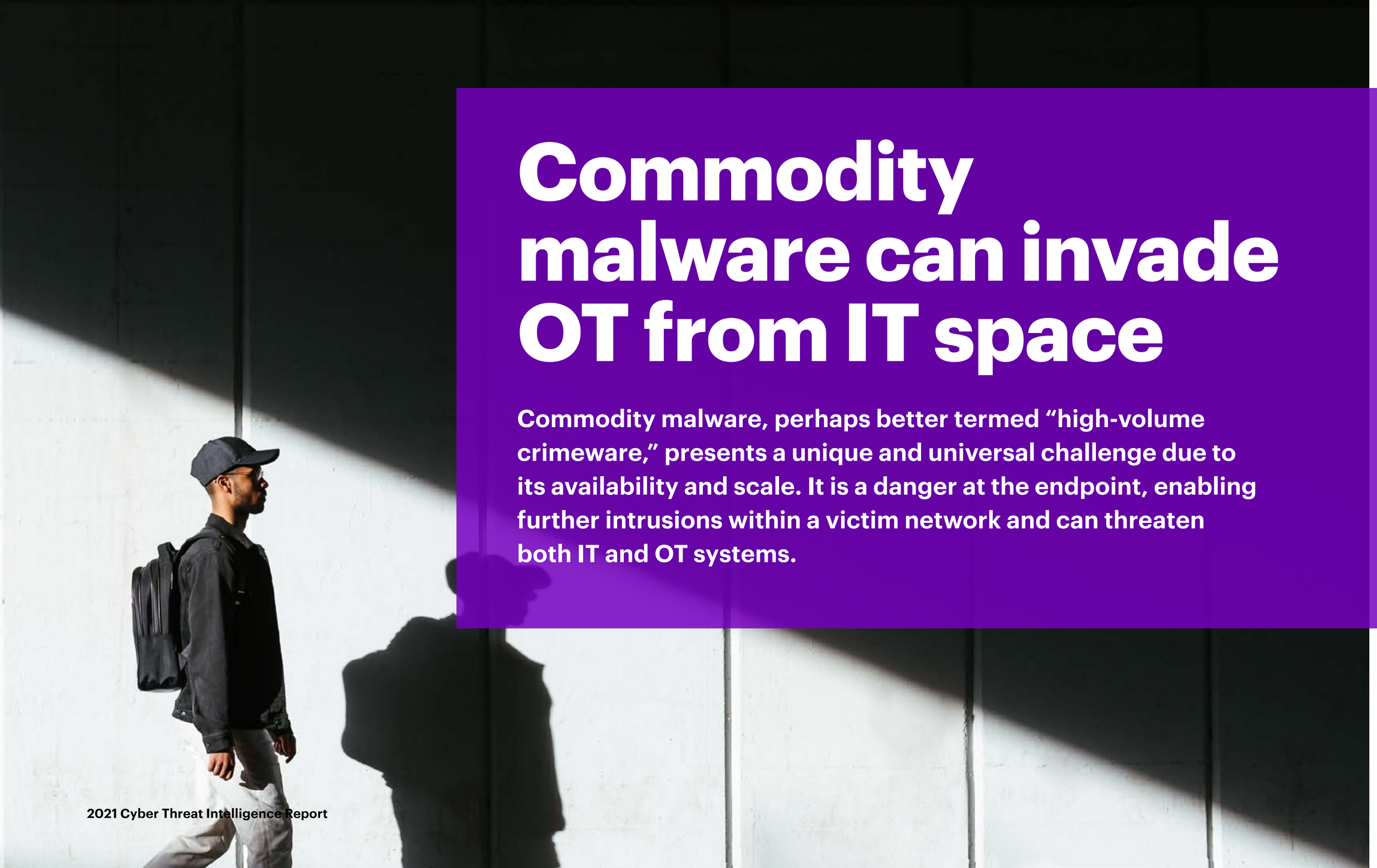
Accenture CTI also observed a Cobalt Strike Beacon-type payload in malware hosted on infrastructure, likely associated with the newly identified cyber espionage group HAFNIUM.[33] HAFNIUM reportedly used zero-day exploits against critical Microsoft Exchange vulnerabilities, which Microsoft publicly disclosed in March 2021.[34]

Malware is merging
Accenture CTI has identified overlaps between the infrastructure of the information-stealing malware EvilGrab and Cobalt Strike Beacon in early 2021 activity.[35] There is a realistic possibility the observed overlaps between EvilGrab and Cobalt Strike are precursors for sophisticated groups that have used EvilGrab in the past adopting Cobalt Strike against new target sets in the remainder of 2021.

Where next?

To help tackle the impact of threats to testing frameworks:

- **Undertake network analysis:** Monitor for discovered Beacon watermarks in Cobalt Strike samples to find and understand emerging Cobalt Strike campaigns and better defend against trending TTPs.
- **Get familiar with Cobalt Strike activity:** Learn how past experiences can help to tackle the threat.
- **Strengthen your defense posture:** Employ new defense tools to keep pace with evolving challenges.



Commodity malware can invade OT from IT space

Commodity malware, perhaps better termed “high-volume crimeware,” presents a unique and universal challenge due to its availability and scale. It is a danger at the endpoint, enabling further intrusions within a victim network and can threaten both IT and OT systems.

QakBot, IcedID, DoppelDridex, and Hancitor are examples of commodity malware threats active in February and March 2021. Accenture CTI's underground reconnaissance team has seldom, if ever, seen threat actors sell these malware types on the Dark Web because relevant threat actors hold onto the malware closely, reducing opportunities to identify spam campaigns early.

Organizations need to consider prevention, rather than response, as the most effective defense against commodity malware threats.

What's happening?

First-stage commodity malware is a notable threat because it enables the deployment of further malware at the endpoint. Threat actors' use of follow-on commodity malware or tools, such as pirated and abused Cobalt Strike instances, increases the risk of an infection spreading throughout an organization's infrastructure and even to OT assets.

Here are some of the active malware campaigns observed by Accenture CTI:

Qakbot and IcedID

According to Accenture CTI research, in March 2021, threat actors used large-volume spam campaigns to deliver crimeware via compressed Excel documents. The embedded malicious macros from the Excel documents download crimeware from URLs with paths that end with "[0-9]{5},[0-9]{9,10}.dat." In a sample activity set, Accenture CTI analysts saw the download of both Qakbot and IcedID payloads during these campaigns. A high percentage of the payloads were Qakbot, an enduring malware that dates back to 2007 that can act as a backdoor. The IcedID Gziploader DLL sends information from the victim system to its C2 server along with the IcedID HTTP cookie parameters "__gads" and "_gat", and the C2 server sends back the IcedID main payload, which is a banking Trojan that also acts as a downloader to deploy follow-on malware.[36]

DoppelDridex

A noteworthy spam campaign in March 2021 lured users with an e-mail that appeared to be from intuit[.]com. E-mails from this campaign have included subjects like "Invoice/Sales Receipt" and "Purchase Order Receipt" and attachments with names like "Payment_Receipt [number].xls." The malicious Excel attachment contains two hidden sheets with invisible strings in cell A15. Upon execution, a macro decodes multiple URLs, downloads the DoppelDridex loader from the URLs and executes it via the Windows regsvr32 process; then the loader drops the embedded DoppelDridex malware into memory and executes it.[37] Threat actors that split from the group responsible for Bitpaymer and Dridex allegedly originated the DoppelDridex malware.[38]

Hancitor

In February and March 2021, spam campaigns delivered the commodity malware Hancitor. Actors spread Hancitor via e-mails with a DocuSign order theme and links to Google Docs URLs hosting malicious Microsoft Word documents. The Word documents dropped an embedded Hancitor DLL to victim systems. Hancitor contacts the C2 domain api.ipify[.]org to report the target machine's external IP address, contact its C2 at URLs using the path "/8/forum.php," and download Ficker Stealer from .ru domains. Hancitor may also deliver the Cobalt Strike malware if the victim system has a Microsoft Active Directory environment.[39] Hancitor activity is connected to the threat group MAN1, a criminal enterprise that Accenture CTI has linked to the Dyre banking malware.[40]

Where next?

To help tackle the impact of commodity malware in OT environments:

- Patch endpoint systems, firewall potential infection vectors, update anti-virus software, keep offline or air-gapped backups and use application whitelists.
- Conduct regular phishing awareness programs for all staff, segment Active Directory domains by function or criticality and maintain a principle of least privilege for each user group and account.
- Remove or disable commonly abused and non-essential services, if appropriate.

Dark Web actors challenge IT and OT networks

Dark Web activities, including enablement of CLOP and Hades ransomware actors, information stealers and digital fingerprints in the underground Genesis Market, reflected noteworthy challenges to both IT and OT networks in early 2021.

Dark Web activities, including enablement of CLOP and Hades ransomware, information stealers and fingerprints in the underground Genesis Market, reflected noteworthy challenges to both IT and OT networks in early 2021.

As threat actors congregate in Dark Web forums to share and trade tools, TTPs and victim data, they are increasing their pressure tactics, learning how to bypass security protections and finding new ways to monetize malware logs.

Organizations need to share information among defenders to understand, prevent, identify and respond to threat activity.

What's happening?

CLOP and Hades ransomware actors are changing the game

Public reporting in early 2021 tied CLOP ransomware actors to a series of global data breaches exploiting a recently discovered vulnerability in the widely used Accellion File Transfer Appliance (FTA).[41] After a review of the timeline of Accellion FTA compromises, CLOP name-and-shame releases on the Dark Web, victim disclosures and insights from Accenture incident response efforts, Accenture CTI agrees that CLOP ransomware actors likely teamed up with the actors responsible for exploiting the Accellion FTA vulnerability.[42] [43] [44] [45] Profitability and managing victims at scale could result in escalation and copycats over the course of the year.

Hades ransomware actors also gained traction in early 2021 and demonstrated their ability to bypass Endpoint Detection and Response (EDR) tools[46] and reach edge devices.[47] Hades actors manually disabled or used custom tools to evade defenses and this skillset could threaten OT networks.[48] Given the EDR bypass, Accenture CTI considers Hades ransomware actors the latest gang threatening both IT and OT networks. Operators' schemes now encompass capturing and encrypting company data and traversing IT networks to OT networks.

Ransomware operators rarely succeed when they try to compromise OT networks, but may not even need to do so to achieve their objectives. In both a February 2021 attack on boat builder Beneteau and the May 2021 Colonial Pipeline attack, the mere presence of actors within the IT network forced preventive OT shutdowns and short-term effects comparable to an OT infection. OT shutdowns, even if preventive, may become more common in future attacks against OT-dependent organizations.[49] [50]

Information is easy to buy and even easier to use

Since the beginning of 2021, Accenture CTI observed a slight but noticeable increase in threat actors selling malware logs, which constitute data derived from information stealer malware.[51] Information stealers can collect and log a wide range of sensitive system, user and business information, such as the following:

- System information
- Web browser bookmarks
- Web session cookies
- Login credentials (websites, Remote Desktop Protocol (RDP), Secure Shell Protocol (SSH))
- Payment card data
- Cryptocurrency wallet addresses

A threat actor can use malware logs to masquerade as a legitimate network user and avoid detection, gaining initial access to a victim system by using valid credentials. Threat actors often use malware logs to access an organization's Web resources and attempt to access privileged administrator accounts on an organization's webservers. In some cases, they may try to access computers on a victim's network via services like RDP or SSH. A common alternative action is for threat actors to sell malware logs directly to hackers, or to sell them in bulk to "malware log" Dark Web marketplaces, such as Genesis Market or Russian Market.

Accenture CTI considers the malware logs that Dark Web actors sell in Genesis Market to pose a particularly serious threat to organizations' IT and OT assets. Genesis Market has drastically lowered barriers to entry for malware log exploitation by compiling and selling malware logs in a format Genesis ads dub "bots" or a "plug-ins." Even less technically savvy threat actors can intuitively use a plug-in with Genesis' freely available Web browser.

Where next?

To help tackle the impact of the Dark Web on OT networks:

- **Undertake responsible monitoring:** Seek early warning of potential unauthorized access through responsible Dark Web monitoring, whether directly or through a cyber threat intelligence provider.
- **Increase intelligence sharing of incident response analysis:** Share information to identify threat signatures and attribution, plan and execute defense and response and prepare network defense and business operations for future threat activity.
- **Prepare a continuity of operations plan:** Anticipate and develop contingency plans for a potential theft of administrator credentials, a bypass of Endpoint Detection and Response systems and physical shutdowns (either as preventive or reactive measures), to prepare network and business operations for the future occurrence of a ransomware or similar event.

Spotlight: On the edge of security

Edge devices such as Internet of Things (IoT) objects, switches and routers operate at the boundary of a network to control data flowing in and out of the organization. At the border between IT and OT environments, they are critical to OT security—breaches can mean direct access into OT environments, completely bypassing IT networks.

But low rates of network monitoring[52] make it difficult for OT incident responders to identify attack vectors and causes of intrusion—and unable to advise on how to secure OT systems. As a result, securing edge devices has become as important as securing ICS themselves.

Policy matters. On December 4, 2020, former President Trump signed the Internet of Things Cybersecurity Improvement Act of 2020.[53] The act encourages government agencies to work collaboratively so that IoT security policies are consistent with National Institute for Standards and Technology (NIST) recommendations.[54] The law promises greater security for edge devices and addresses some longstanding challenges. On May 12, 2021, **President Biden signed the Executive Order on Improving the Nation's Cybersecurity** which includes direction to create pilot cybersecurity labelling programs to educate the public on security capabilities of IoT devices and software development practices.[55]

Stringent edge device policies may encourage organizations to allocate funds from many parts of the business to bolster security efforts. With investment in the right places, security leads can secure edge devices in OT environments through a combination of monitoring, response and intelligence.

Targeting edge devices

In February 2021, Accenture CTI discovered a threat actor advertising Citrix VPN access to a “large resources corporation” on a reputable Russian-language forum specializing in malware and ransomware.[56] Citrix is a VPN gateway commonly placed at OT boundaries to connect and correlate various Internet protocols from different networks.

Threat actors often access vulnerable networks and systems such as Citrix by exploiting known vulnerabilities that are unpatched or that vendors are in the process of patching. In late 2019, the still-active threat campaign known as Fox Kitten (also known as UNC757)[57] accessed companies in various industries, including the energy industry, via VPN n-day exploits.[58]

Financially motivated cyber criminals have used VPN access to launch a ransomware attack and may target OT systems—they know manufacturers and other users of ICS are especially vulnerable to downtime and may be more likely to pay ransoms to get their systems back online.

Meanwhile, cyber espionage threat actors may use VPN access to get onto OT networks to steal data or hide with the intention of issuing a destructive attack later. Both threat actor types can access edge devices, which could lead to the disruption of critical business operations and loss of revenue.

Defend the edge

Here are some familiar security capabilities organizations can use to increase their edge device security:

OT Security Operations Center (SOC)
Unlike a traditional SOC that focuses primarily on IT assets, an OT SOC monitors security events in both the IT and OT environments for visibility of threats and risks. Monitoring edge devices on the boundary of an OT environment is a key component of overall cybersecurity and cyber resiliency. An OT SOC coupled with managed detection and response (MDR) can help defend against cyber threats and reduce exposure to them.[59]

OT Incident Response (IR)
OT IR is essential in uncovering how threat actors access OT environments via edge devices if a breach occurs. Insight into how threat actors access edge devices and traverse into an OT environment enables an entity to secure its IT and OT boundaries. Data from OT IR engagements can also help inform red teaming exercises to identify edge vulnerabilities before an edge breach occurs. OT IR is a key component of security in the context of OT and IT convergence, as well as operational security as a whole.

Cyber Threat Intelligence (CTI)
Traditional cyber threat intelligence provides information on threat actors targeting IT or OT, but often only addresses edge device security during the deployment of highly specialized systems. Accenture CTI takes OT security a step further with key vulnerability intelligence and monitors major edge devices, their vendors and their version numbers to make clients aware of threats to IT, OT and cloud environments.

Cyber threat intelligence offers improved visibility into overall network threats and informs decision makers how to prioritize security around potential targets and threats.

As edge device vulnerabilities and targeting are on the rise, it is critical for organizations to start changing their security cultures from being reactive to adopting a proactive approach to security “on the edge.”

References

1. Eaton, Collin and Volz, Dustin, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," Wall Street Journal, May 19, 2021.
2. "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware, February 1, 2021.
3. "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound," Coveware, April 26, 2021.
4. "2020 Cyber Threatscape Report," Accenture, October 19, 2020. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion," Accenture, December 15, 2020.
5. Accenture Cyber Threat Intelligence, "Ransomware Roundup from iDefense Analysis," April 8, 2021. IntelGraph reporting.
6. Accenture Cyber Threat Intelligence, "Ransomware Attack on Cyber Insurer Highlights Risks to Cyber Insurance Sector and its Customers," April 8, 2021. IntelGraph reporting.
7. Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak CGG Data on Name-and-Shame Site on 1 March 2021," March 10, 2021. IntelGraph reporting; Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak CSX Documents on Name-and-Shame Site on 2 March 2021," March 10, 2021. IntelGraph reporting.
8. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion," December 15, 2020, Khodzhibaev, Azim et al, "Interview with a Lockbit Ransomware Operator," Talos, January 4, 2021.
9. "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware, February 1, 2021. The average paid ransom declined 34%, from US$233,817 in Q3 to US$154,108 in Q4. "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound."
10. Moore, Andrew et al, "Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion," February 22, 2021. FireEye; Accenture Cyber Threat Intelligence, "SITREP: Accellion FTA," February 20, 2021. IntelGraph reporting.
11. Accenture Cyber Threat Intelligence, "Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect," November 6, 2020. IntelGraph reporting.
12. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion," December 15, 2020.
13. "What We Know About the DarkSide Ransomware and the US Pipeline Attack," TrendMicro, May 12, 2021.
14. Accenture Cyber Threat Intelligence, "Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect," November 6, 2020. IntelGraph reporting.
15. Mansfield, Paul. "Tracking and combatting an evolving danger: Ransomware extortion." December 15, 2020.
16. Accenture Cyber Threat Intelligence, "iDefense Global Research Intelligence Digest for 31 March 2021," March 31, 2021. IntelGraph reporting.
17. Abrams, Lawrence, "Ransomware gang plans to call victim's business partners about attacks," March 6, 2021. Smilianets, Dmitry, "'I scrounged through the trash heaps... now I'm a millionaire:' An interview with REvil's Unknown," March 16, 2021.
18. "FBI Statement on Compromise of Colonial Pipeline Networks," FBI, May 10, 2021.
19. "What We Know About the DarkSide Ransomware and the US Pipeline Attack," Trend Micro, May 14, 2021.
20. Cimpanu, Catalin, "Some ransomware gangs are going after top execs to pressure companies into paying," January 9, 2021.
21. Accenture Cyber Threat Intelligence, "Transparency Activists Publicize Ransomware Victims' Data in a New Twist on Hybrid Financial-Political Threat," January 8, 2021. IntelGraph reporting.
22. Accenture Cyber Threat Intelligence, "Colonial Pipeline Attack Impacts Ransomware Groups Operating on the Dark Web," May 17, 2021. IntelGraph reporting.
23. Ilascu, Ionut, "Hackers use black hat SEO to push ransomware, trojans via Google," Bleeping Computer, March 1, 2021.
24. Welling, Eric, "It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims," Accenture, March 26, 2021.
25. Michael, Melissa, "Episode 49| Ransomware 2.0, with Mikko Hypponen," F-Secure, January 19, 2021.
26. Toby L, "The rise of ransomware," National Cyber Security Centre, January 29, 2021.
27. "Adversary Infrastructure Report 2020: A Defender's View," Recorded Future, January 7 2021.
28. Cunliffe, Amy, "The development of Mimir (Amy Cunliffe, Accenture)," CREST Videos, April 9, 2021.

29. "Threat Landscape Trends – Q3 2020," Symantec, December 18, 2020.

30. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," FireEye, December 13, 2020.

31. "Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop," Microsoft, January 20, 2021.

32. Welling, Eric, "It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims," Accenture, March 26, 2021.

33. Accenture Cyber Threat Intelligence, "Microsoft Exchange On-Premise Zero-Day Vulnerabilities Related Malware Activity in March 2021," March 10, 2021. IntelGraph reporting.

34. "HAFNIUM targeting Exchange Servers with 0-day exploits," Microsoft, March 2, 2021.

35. Accenture Cyber Threat Intelligence, "EvilGrab and Cobalt Strike Beacon Observed having Shared Infrastructure and Communicating," February 3, 2021. IntelGraph reporting.

36. Accenture Cyber Threat Intelligence, "Spam Campaign Distributes Gziploader to Deploy IcedID (a.k.a. BokBot) Malware in March 2021," April 14, 2020. IntelGraph reporting.

37. Accenture Cyber Threat Intelligence, "Technical Analysis of DoppelDridex," April 27, 2021. IntelGraph reporting.

38. Stone-Gross, Brett; Frankoff, Sergei; and Hartley, Bex, "BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0," July 12, 2019.

39. Accenture Cyber Threat Intelligence, "iDefense Global Research Intelligence Digest for 6 April 2021," April 6, 2021. IntelGraph reporting.

40. Accenture Cyber Threat Intelligence, "MAN1," July 16, 2016. IntelGraph reporting.

41. Seals, Tara, "Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11," Threatpost, February 22, 2021.

42. Accenture Cyber Threat Intelligence, "SITREP: Accellion FTA," March 5, 2021. IntelGraph reporting.

43. Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak Qualys Documents on Name-and-Shame Site on 3 and 4 March 2021," March 4, 2021. IntelGraph reporting.

44. Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak CGG Data on Name-and-Shame Site on 1 March 2021," March 10, 2021. IntelGraph reporting.

45. Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak CSX Documents on Name-and-Shame Site on 2 March 2021," March 10, 2021. IntelGraph reporting.

46. Welling, Eric, "It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims," Accenture, March 26, 2021.

47. Accenture Cyber Threat Intelligence, "Hades Ransomware Affects Large Corporate Networks from December 2020 to March 2021," April 9, 2021. IntelGraph reporting.

48. Accenture Cyber Threat Intelligence, "Hades Ransomware Affects Large Corporate Networks from December 2020 to March 2021," April 9, 2021. IntelGraph reporting.

49. Arghire, Ionut, "Boat Building Giant Beneteau Says Cyberattack Disrupted Production," Security Week, March 1, 2021.

50. Bertrand, Natasha et al, "Colonial Pipeline did pay ransom to hackers, sources now say," CNN, May 13, 2021.

51. Accenture Cyber Threat Intelligence, "Monthly Reconnaissance Report," April 1, 2021.

52. Filkins, Barbara, Wylie, Doug, "SANS 2019 Sate of OT/ICS Cybersecurity Survey," SANS, June 2019. Slightly over 50% of survey respondents reported continuous monitoring to detect vulnerabilities, and only 1/3 of 25 surveyed OT/ICS security monitoring technologies were in use across all respondents.

53. United States Congress, "PUBLIC LAW 116–207—DEC. 4, 2020," December 4, 2020.

54. United States Congress, "PUBLIC LAW 116–207—DEC. 4, 2020," December 4, 2020.

55. The White House, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021,

56. Accenture Cyber Threat Intelligence, "Threat Actor … Advertise Compromised Citrix Access to Three Large Corporations," February 26, 2021, IntelGraph reporting.

57. "Groups," MITRE, accessed May 27, 2021.

58. "Fox Kitten Campaign," Clearsky Cyber Security, February 16, 2020.

59. "Managed Security," Accenture, accessed April 4, 2020.

Contacts

Joshua Ray
Managing Director
Accenture Security

Josh Ray is Managing Director for Cyber Defense across Accenture globally. Josh has more than 20 years of combined commercial, government and military experience in the field of cyber intelligence, threat operations and information security. He holds a Bachelor of Science degree in information technology from George Mason University, an Executive Certificate in strategy and innovation from MIT Sloan School of Management and served honorably as a member of the United States Navy.

Howard Marshall
Managing Director
Accenture Security

Howard Marshall is Managing Director for Accenture Cyber Threat Intelligence (CTI) and leads the business globally. Prior to joining, Howard was FBI Deputy Assistant Director of the Cyber Readiness, Outreach and Intelligence Branch. He holds a Bachelor of Arts degree in Political Science and a Juris Doctorate from the University of Arkansas.

Jayson Jean
Senior Manager
Accenture Security

Jayson Jean is Director of Business Operations for Accenture CTI in North America and the Asia Pacific region, with responsibility for business development of the Cyber Threat Intelligence portfolio. Prior to this role, Jayson has 14 years of experience building the strategic direction and leading product development for vulnerability management at Accenture CTI.

Christopher Foster
Senior Principal
Security Innovation

Chris Foster is Director of Product Strategy for Accenture Cyber Threat Intelligence. Chris has more than 18 years of combined experience in the field of threat intelligence serving public and private sector organizations to include Booz Allen Hamilton, Chevron, United States Department of Defense and United States Department of Homeland Security. He holds a Bachelors from Vanderbilt University and an MBA from the McCombs School of Business, University of Texas at Austin.

Valentino De Sousa
Senior Principal
Security Innovation

Valentino De Sousa leads Accenture Cyber Threat Intelligence in Europe. He is a member of the ENISA Ad-Hoc Working Group on Cyber Threat Landscapes. Previous roles include leading different threat intelligence teams responsible for malware analysis, research and development, analysis of adversaries, active campaigns and leading indicators of impeding attacks. He holds a Bachelor of Science in business administration from the American University of Rome and a Master of Science in terrorism studies from the University of East London.

Contributors

Patton Adams, Will Archer, Adam Bumgarner, Bianca Forbes, Roya Gordon, Hannaire Mekaouar, Nellie Ohr, Max Smith, Nancy Strutt.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 569,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. **Visit us at www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. **Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security**

210353