Threats Unmasked

Cyber Threat Intelligence Report

Volume 2 – 2021

accenture

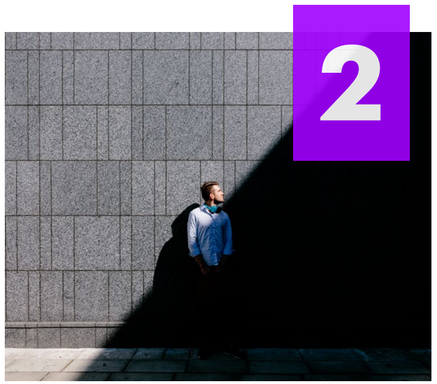
Accenture has been creating relevant, timely and actionable threat intelligence for more than 20 years. Our cyber threat intelligence and incident response team is continually investigating numerous cases of financially motivated targeting and suspected cyber espionage.

During these investigations, our threat intelligence and incident response analysts have gained firsthand visibility into the tactics, techniques and procedures (TTPs) employed by some of the most sophisticated cyber adversaries. This report reflects analysis during the second half of calendar year 2021 (H2 2021).

Key trends

Following analysis in H2 2021, Accenture identified five trends affecting the cybersecurity landscape:

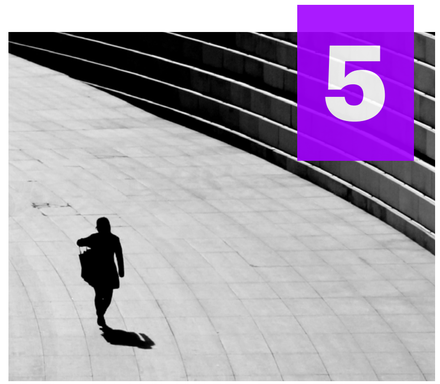
Ransomware attacks still prove profitable



Supply chains offer attack footholds

Information stealers boost the malware market

Cloud-centricity prompts new attack vectors



Vulnerability exploits see high volume buying and selling

Ransomware attacks still prove profitable

Despite technology enabling threat actors to become even more sophisticated, there are still active and evolving risks from tried and tested ransomware techniques. And there is consistency of ranking for the top targeted industries throughout Q3 of calendar year 2021, with ransomware threat actors proving most successful against the manufacturing industry, followed by financial services, healthcare, technology and construction.

Ransomware attacks continued to be profitable; among the most active ransomware groups in 2021 were LockBit and Conti, but tracking individual groups remains challenging due to continuous “retirements” and rebranding into new groups due to law enforcement pressure or internal group dynamics.

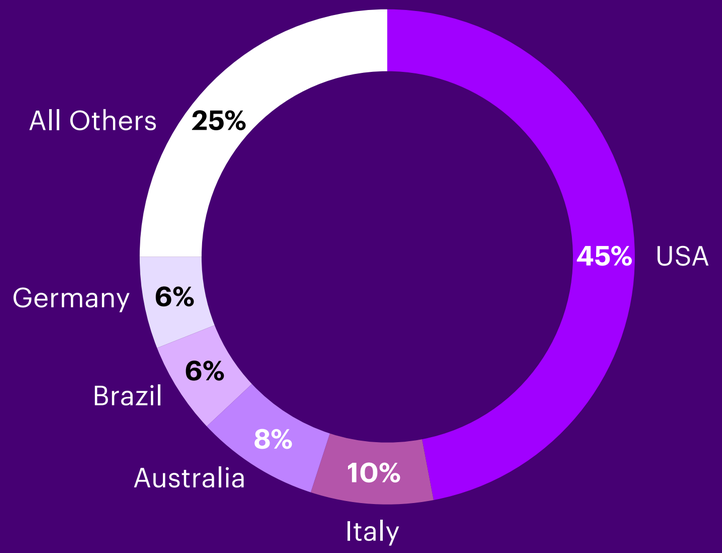
Conflict between ransomware affiliates and their operators led to information leaks. Arguments between involved parties serve as one example of the unintended consequences of ransom-affiliate payment schemes. Despite these problems, ransomware operations remain highly profitable.

What is more, increasingly, ransomware operators abused cloud infrastructure and introduced new encryption techniques to better evade detection and increase impact.

Based on data collection from Accenture incident response engagements, ransomware and extortion operations made up almost 35% of intrusion volume in 2021 and represented a 107% year-over-year increase from 2020.

In addition, the United States was again the top region impacted by ransomware and extortion threats, representing approximately 45% of intrusion volume in 2021 (Figure 1).

Figure 1. Ransomware by geography (Incident response)

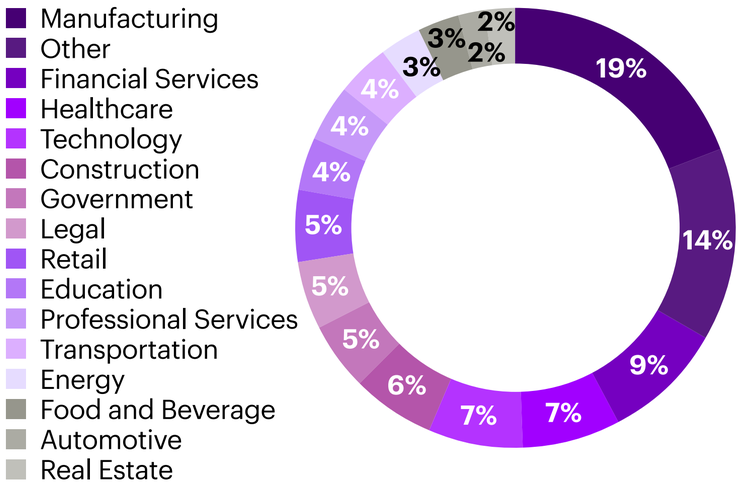


What's happening?

Top four industry targets remain the same

The number of ransomware attacks decreased slightly in Q3 compared to Q2 of calendar year 2021, with manufacturing, financial services, healthcare and technology remaining the most targeted industries. Targeting against the construction sector increased, making it the fifth-most-targeted industry during Q3 (see Figure 2).

Figure 2. Top 15 industries targeted by ransomware in Q3 2021



New RAMP forum creates rampage

Following the DarkSide group's dissolution after the Colonial Pipeline attack,[1] the Groove ransomware collective emerged in September 2021 and created the RAMP forum, which connects orphaned affiliates with ransomware-as-a-service (RaaS) operators. This forum's emergence could mean there is continued growth for RaaS activity and poses a significant and continuing threat to businesses.

Media reporting increases impact

Active media reporting reflects a "scoop-and-scandal"-driven culture in the cybersecurity community and unintentionally increases cyber threat actors' influence. Cyber criminals used this publicity in Q3 calendar year 2021 to criticize rivals and increase pressure on victims.

Affiliate disputes are on the rise

There's a growing number of disputes between ransomware affiliates and ransomware group operators. Former affiliates of ransomware groups disclosed sensitive information, leading to a proliferation of potent ransomware tools and techniques.

Attack playbook isn't the whole story

The Conti Playbook—an attack playbook disclosed by a former member of the Conti ransomware threat group—suggests Conti affiliates tend to use options like well-established cybercrime botnets, malicious spam and spear phishing.

Cloud plays into ransomware's hands

Cloud environments were and continue to be attractive targets, perhaps due to lower monitoring levels than on-premise environments. In this way, cloud-related malware has evolved faster than more

traditional malware in 2021 based on analysis of the rate of code changes between cryptominers (a primary malware malicious actors deploy in compromised cloud environments) compared to code changes in botnets and ransomware. This comparison of the rate of code change highlights significant threat actor investment in cloud-focused tools—particularly in modifying pre-existing tools.[2]

During multiple incident response engagements in 2021, Accenture observed ransomware and extortion operators targeting cloud infrastructure and hosted backups in attempts to increase operational impact. This included exploitation of SAML (Security Assertion Markup Language 2.0) identity federation in use to access Amazon Web Services (AWS) via Microsoft Azure Active Directory (Azure AD), using previously compromised credentials to enable unauthorized console access to several AWS resources and support further objectives.[3] At least one ransomware group used an offensive cloud toolset that vx-underground researchers leaked from threat group TeamTNT in October 2021; this toolset specializes in cryptojacking operations. This use indicates a trend of ransomware groups' custom tool development for increased cloud infrastructure targeting.[4]

Underground forum members are trading in endpoint accesses

Underground forums are showing increased interest in accessing compromised virtual private networks (VPNs) via stolen credentials and the use of public and zero-day exploits.

For example, Accenture analysis of September to November 2021 network access seller data shows malicious actors selling victim network accesses on underground forums gained almost all those accesses via VPNs whose credentials were compromised and used by threat actors to authenticate.[5]

Data extortion is rising without ransomware deployment

In the second half of 2021, Accenture observed **new threat groups** establishing infrastructure and ramping up attacks solely focused on data exfiltration and extortion rather than more destructive ransomware deployments. We expect to see this trend continue to rise in Q1 CY2022, as this simplified approach enables the execution of attacks and subsequent extortion attempts more quickly and at scale.

Actors infer insidious insiders

Along with an unsubstantiated claim of insider access at Accenture, actors using LockBit implied in November 2021 they have an insider at another major corporation.[6] Robust insider threat programs can help to quickly confirm or refute threat actor claims which may be intended to deceive responders. This can backfire on threat actors as it can lower their credibility and therefore their chances of obtaining ransom payments.

Where next?

Here are some ways to defend against ransomware attacks:

- Build zero trust principles into the organization's security strategy to secure customer and corporate data.
- Establish and exercise a business continuity of operations (COOP) plan which builds resiliency into the corporate response and includes public messaging, internal communications, and enforce a policy of robust offsite backups.
- Implement a measurable security training and awareness program which focuses on educating users to think twice before clicking on links and to identify and safely report emails that could be part of a phishing campaign.
- Establish an asset management program that includes an inventory of remote desktop protocol (RDP) solutions and the implementation of secure and monitored VDI solutions. Limit the use of RDP, close unused RDP ports, apply two-factor authentication, and log RDP logon attempts.
- Manage cloud assets by monitoring end points and ensuring process visibility.
- Regularly patch operating systems, software and firmware.
- Incorporate response plans for malware or wiper attacks into the organization's COOP plan.
- Incorporate intelligence into the organization's cyber defense strategy to monitor dynamics within threat groups, underground forums, and evolving TTPs to update detection and response countermeasures.
- Reject ransom demands—the United States government encourages ransomware victims to refuse ransom demands, as ransom payments only encourage threat actors to attack again. Organizations that choose to pay a ransom should:
  - Immediately report the incident to law enforcement and the Cybersecurity and Infrastructure Security Agency (CISA).
  - Cooperate with law enforcement throughout the incident recovery process
  - Implement a sanctions compliance program to properly assess the risks. If the ransom group is a sanctioned entity, contact the Office of Foreign Assets Control (OFAC) immediately.
  - Understand a ransom payment does not guarantee regaining access to locked machines or data.

Supply chains offer attack foothold

Since the revelation of the SolarWinds supply chain campaign in December 2020,[7] increasingly, malicious operators have realized the potential of supply chain attacks. In addition to the complexities of asset and vendor management and visibility into software bill of materials, moving to the cloud has meant many organizations further increased the risk and consequences of supply chain insecurities. Such vulnerabilities can result from potential supply chain incidents across entire on-premise and cloud environments serving one or multiple business entities.

What's happening?

Widely reported threat increases

During October and November 2021, numerous cybersecurity publications mentioned supply chain attack campaigns referencing developer library and software platform compromises.

Backdoor threats are more prevalent

In the same timeframe, Accenture noted references to at least nine malicious node package managers (NPMs) masquerading as legitimate packages. There were also two legitimate NPM packages with backdoors built into them that enable a threat actor to bypass normal authentication channels and interactively issue commands to a system.[8] NPM is a center for JavaScript code-sharing in wide use by software developers.

Some NPM code packages are downloaded millions of times every week. A package with a backdoor and a download cadence that high could provide initial attacker footholds on thousands of victim networks or cloud tenants. Malicious actors can use such footholds for a wide variety of purposes, including cryptojacking,[9] espionage,[10] ransomware deployment and destructive wiper attacks.[11]

Based on intrusion data Accenture collected from incident response engagements, 30% of the malware threats Accenture observed in 2021 were backdoor threats, making them the second-most-prevalent type of malware, behind ransomware (33%).

Where next?

Here are some ways to counter the threat of supply chain attacks:

- **Integrate audits:**
  Administrators should integrate audits into DevOps cycles. The need to weave security into both DevOps and application onboarding has catalyzed the integration of platforms for automated code scanning. These include intelligent and integrated platforms that help organizations develop code more quickly with lower remediation costs, higher security and fewer staff. For example, the **Accenture Intelligent Application Security Platform** enables developers and team leads to build security into full application life cycles, from development to testing and deployment, as well as to remediate code base vulnerabilities automatically.[12]

- **Update security frameworks**:
  Administrators should either adopt standards and use monitoring tools to meet compliance demands or enroll in application security as-a-service offerings to block malicious actors' direct access to sensitive environments and repositories, such as developer machines and source-code repositories. In the SolarWinds supply chain attack, malicious actors used a position on developer machines to inject malicious code into the SolarWinds Orion platform before Orion developers compiled and digitally signed the Orion software.[13] Such incidents underline the importance of application security and the severe penalties of failure.

- **Threat-modeling suppliers:**
  Administrators and security personnel should look beyond software and examine their organizations' broader third-party dependencies.

- **Mature software supply chain programs:**
  To reduce risks associated with software supply chains, consider the following guidance:

  - **Refer to the "Best Practices in Cyber Supply Chain Risk Management"** document from the National Institute of Standards and Technology for information on mapping supply chains, identifying critical suppliers and reviewing cybersecurity practices for suppliers' personnel.

  - Review the privilege and access levels of externally developed software at an organizational level. Although vetting all software may not be a realistic objective, basic improvements can drastically improve an organization's security posture.

  - Review service-level agreements with software suppliers to actively locate and fix vulnerable software prior to deployment.

Infostealers boost the malware market

The increased popularity of underground endpoint marketplaces that sell packages of compromised login data continues to pose a substantial threat to organizations across industries and geographies. Endpoint marketplaces offer an abundance of inexpensive gateways into corporate networks.

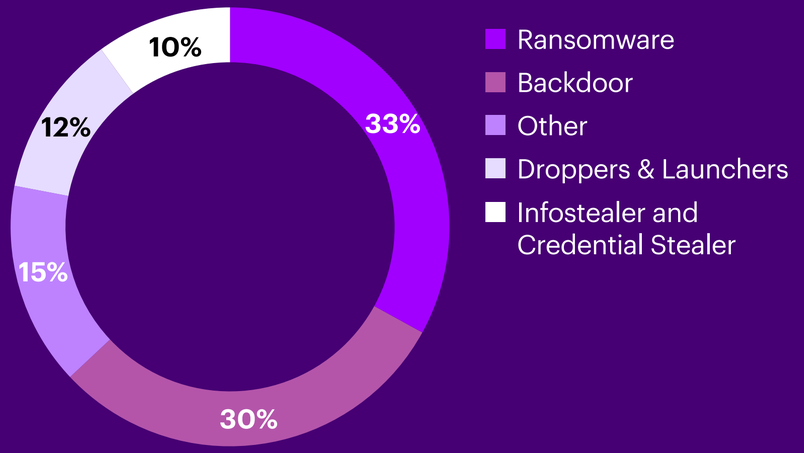
Compromised endpoints—which underground actors have bundled and sold as so-called “bots”—contain login credentials, sensitive system information and cookie sessions. Actors siphon this information from victims’ machines using credential-stealing malware and sell it on Dark Web marketplaces for as little as US$10 to US$200.

Accenture research shows that marketplaces for endpoint access threaten the majority of medium-to-large corporations across industries and geographic regions, which face exposure directly through a corporation’s own networks or through third party compromises.

Information stealers (malicious software known as infostealers) are typically designed to obtain (that is, access or copy) credentials with functionality beyond basic keylogging. This could include usernames, passwords, keys, tokens, cookie sessions and so on.

Based on intrusion data Accenture collected from incident response engagements, the combined infostealer and credential stealer category made up approximately 10% of malware observed during intrusions in 2021 (Figure 3).

Figure 3. Malware by category (Incident response)



What's happening?

Infostealers are highly active

As of November 2021, based on available data, the most utilized infostealers providing underground marketplace inventory are Redline (53%), Vidar (35%), Taurus (4%), Racoon (4%) and Azorult (2%) (see Figure 4).

However, Accenture also found information-stealing campaigns active in June to November 2021 using Qakbot and NanoCore most often (see Figure 5).

Figure 4. Infostealers feeding data to endpoint marketplaces

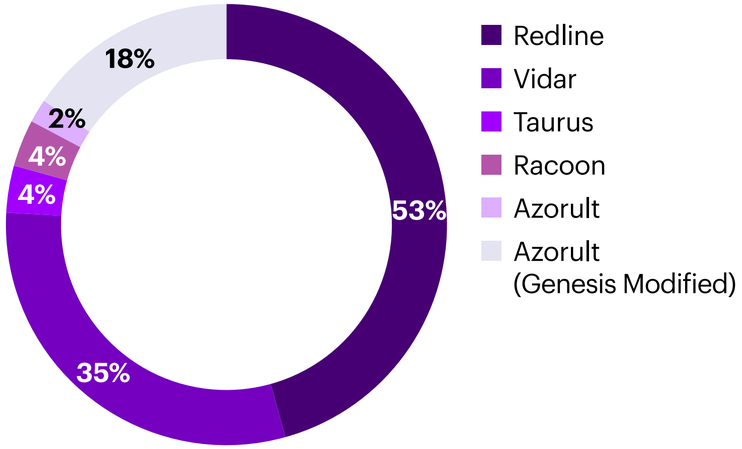
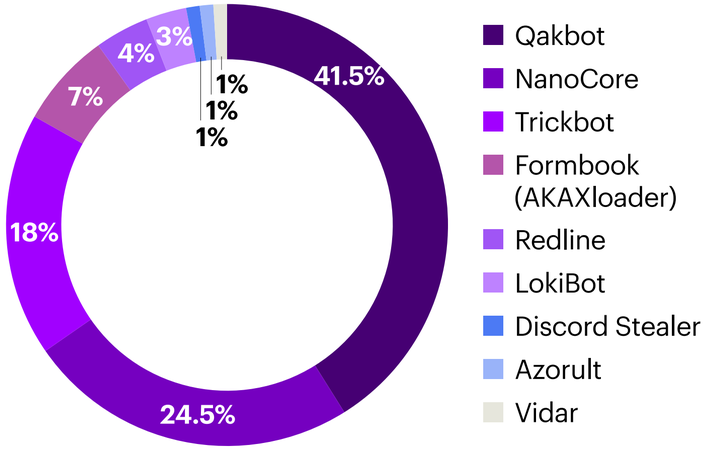


Figure 5. Infostealers used by malicious actors in threat campaigns



Infostealer popularity varies

Data collection biases partially explain the discrepancy between the infostealer actors used in then-active campaigns and those they used to feed marketplaces with inventory. Yet, this inconsistency also showcases underground marketplaces' reliance on newer infostealers, while established groups rely on tried and tested infostealers.

And while Redline only makes up 4% of the market share, the use of this infostealer is growing at a faster rate than the others. Redline has gained popularity following its involvement in the July 2021 Tokyo Olympic ticket data breach.[14] Redline infects systems through a loader installed by malicious Microsoft Word or Excel documents in phishing emails or social media messages.[15]

Where next?

Here are some ways your organization can position itself to address malicious software:

- **Protect corporate environments:** Accenture research shows that while marketplace infostealers have infected both corporate and private machines, the latter creates greater exposure for both if it is able to synchronize with corporate infrastructure. This synchronization enables infostealers to increasingly avoid security measures that strict corporate environments provide and enables infostealers to remain in victims' systems longer, updating scraped information as that information changes over time.
- **Be aware of the growing "bots" business:** The number of so-called "bots" (tools that incorporate the functionality of login credentials, cookie sessions and "plugs" which enable the easy use of stolen data via a browser plug-in) for sale on underground marketplaces has increased steadily since 2017—from approximately 76,000 "bots" for sale between December 2017 and December 2019 to more than 11 million "bots" for sale between December 2019 and November 2021. Accenture attributes this rapid rise to the remote working environment, accelerated by the COVID-19 pandemic and greater use of multi-factor authentication (MFA), which has increased the utility and value of these "bots."

  Depending on a corporation's security posture, these "bots" can grant direct access to affected systems or provide skilled actors an easier way into networks. Stealing an active cookie session makes "bots" significantly more effective than using compromised login credentials alone. As a result, ransomware groups, business email compromise rings and data extortionists commonly use endpoint marketplaces, with Accenture and other cybersecurity organizations attributing multiple recent attacks to the endpoint market.[16]

Cloud-centricity prompts new attack vectors

Increasingly, threat actors are exploiting public-facing cloud infrastructure to deploy offensive toolsets and use internal access points to organizations' cloud environments. This threat is growing as organizations accelerate cloud adoption and open up new attack vectors using, for example, toolsets originally designed for cryptojacking, which an actor can repurpose for other malicious activity. Cryptojacking, also known as cryptomining, hides on a computer or mobile device and uses the machine's resources to "mine" forms of cryptocurrencies.

What's happening?

Rapid cloud growth feeds attack opportunities

The COVID-19 pandemic has accelerated the already ongoing trend of cloud adoption to enable remote working, online education, business resilience and environmental sustainability, opening up new attack surfaces and increasing the value of cloud infrastructure attacks for malicious actors.[17] "Forecasts of global end-user spending on public cloud services show it reaching US$482B in 2022—a 21.7% increase from 2021's expected US$396B.[18]"

Expanding infrastructure opens the door to new vulnerabilities

Some organizations do not monitor cloud platforms as closely as they do their own on-premise servers, which may exacerbate existing deficiencies in cloud asset and configuration management.

Instead, they are placing their trust in a third party cloud provider. As a result, threat actors are hijacking cloud services to exploit cloud infrastructure's benefits, collect sensitive data and deploy ransomware.

Expanding cloud infrastructure also creates highly scalable and reliable command-and-control infrastructure and botnets. Additionally, public-facing cloud environments serve as initial entry vectors through which threat actors can gain access to individual endpoint devices.

Cloud-centric toolset threats are escalating

Accenture has observed a highly evolved and active cloud-centric toolset from TeamTNT, a threat group prolific at mining cryptocurrency through cloud resource exploitation —otherwise known as cryptojacking.

On October 29, 2021, security researchers leaked TeamTNT's toolset for attacking public-facing cloud platforms.[19] Accenture analyzed the leaked TeamTNT scripts and assessed the group likely deployed this toolset as part of numerous cloud-focused cryptojacking operations.[20] These cryptojacking operations include the "Chimaera" campaign, that TeamTNT reportedly oversaw from at least July 2021 and which caused thousands of infections globally.[21]

Beyond cryptojacking activities, TeamTNT's toolset installed a bot named "Tsunami" onto compromised systems. This bot's code base is similar to that of the infamous Mirai malware and can abuse public-facing infrastructure to execute brute-force attacks, run global IP scans and launch distributed denial-of-service attacks.

Once the Tsunami bot infects systems, TeamTNT's toolset can enumerate internal infrastructure and deploy malicious executables, exploiting cloud platforms such as Google Cloud, Amazon AWS, Kubernetes and Dockers within Linux/Unix and Windows environments.

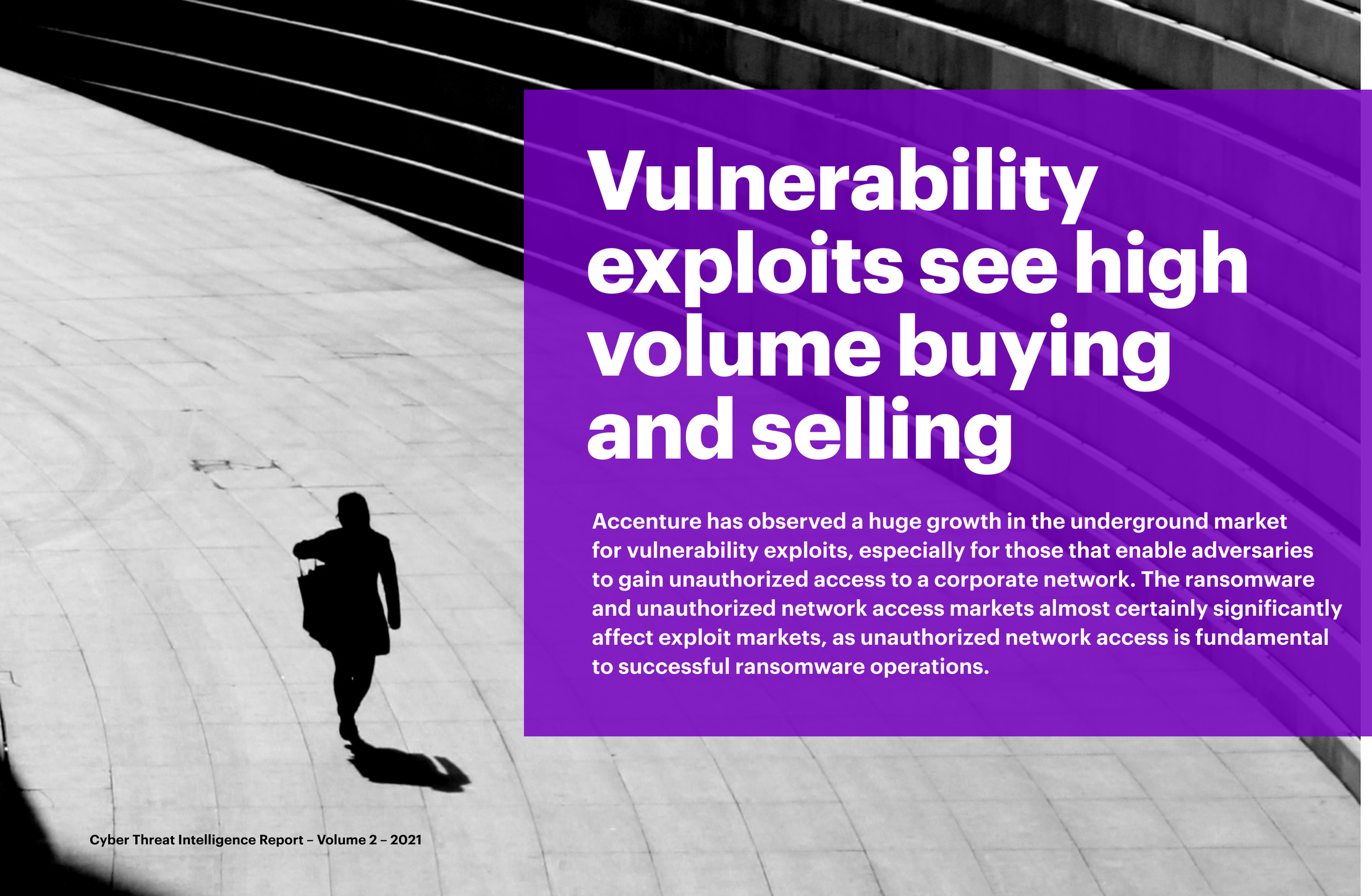
Researchers claim the ransomware extortion groups Conti and DarkMatter are actively using TeamTNT's leaked archive.

Although Accenture has not observed evidence of ransomware affiliates deploying TeamTNT's toolset, Accenture assesses with high confidence that moderately skilled threat actors can easily deploy the toolset's scripts to compromise private cloud entry points and tailor the code's mining functionalities to encrypt data post-compromise. Such adaptation would mark a natural evolution of ransomware campaigns as ransomware groups' interests in cloud infrastructure grows.

Where next?

Here are some suggested ways to mitigate the impact of cloud platform threats:

- **Audit and test for cloud misconfigurations** alongside organizational operation digitalization efforts.
- **Adopt an identity and access management framework** to monitor and control cloud user access permissions.
- **Establish MFA** across cloud access points and monitor virtualization infrastructure access.



Vulnerability exploits see high volume buying and selling

Accenture has observed a huge growth in the underground market for vulnerability exploits, especially for those that enable adversaries to gain unauthorized access to a corporate network. The ransomware and unauthorized network access markets almost certainly significantly affect exploit markets, as unauthorized network access is fundamental to successful ransomware operations.

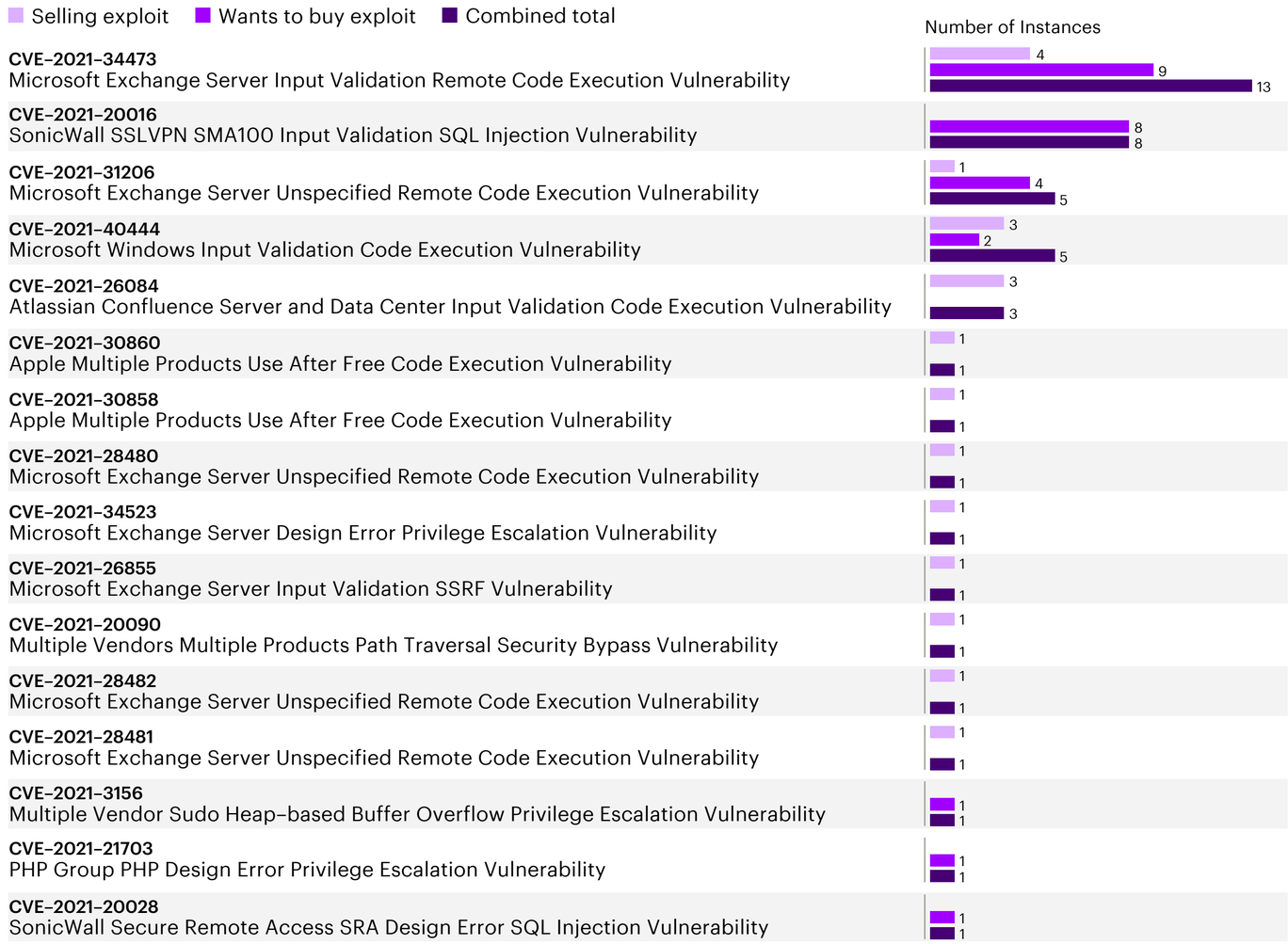
What's happening?

Actors are busy selling or buying CVE exploits

Accenture analyzed 45 instances of underground actors wanting to sell or buy exploits for Common Vulnerabilities and Exposures (CVEs) between August 2021 and October 2021 (Figure 6). We identified:

- 24 actors buying or selling exploits for 16 CVEs across four forums or marketplaces.
- 16 actors wanting to buy exploits for seven CVEs.
- Nine actors selling exploits for 12 CVEs.

Figure 6. Instances of actors buying or selling exploits for CVEs (August–October 2021)



Actors have "top three" vulnerabilities they buy and sell

During the period August – October 2021, the three most popular CVE exploits on the market are for CVE-2021-34473, CVE-2021-20016 and CVE-2021-31206. Accenture analyzed these vulnerabilities in the context of the potential impact of successful exploitation and the assessed intentions of the actors seeking to purchase related exploits.

Accenture found that successful exploitation of each of the noted vulnerabilities enables a remote adversary unauthorized access to a victim network and execution of arbitrary code on a victim host. Analysis of past activities of actors who sought to purchase exploits indicates the actors are financially motivated and that it is likely they intend to use the exploits to facilitate unauthorized network access schemes.

Here is further detail on the most popular CVE exploits:

- **CVE-2021-34473:** Accenture identified two actors selling the same exploit and eight financially motivated actors wanting to buy an exploit for CVE-2021-34473 in the period of August – October 2021. CVE-2021-34473 (also known as ProxyShell) is an improper input validation vulnerability (CWE-20) in Microsoft Exchange Server 2013-2019. An actor chaining CVE-2021-34473 with CVE-2021-34523 and CVE-2021-31207 could execute arbitrary code with SYSTEM-level privileges on a victim host.
- **CVE-2021-20016:** Accenture identified four financially motivated actors wanting to buy a CVE-2021-20016 exploit, but did not identify any actors wanting to sell any. CVE-2021-34473 is a SQL injection vulnerability (CWE-89) in SonicWall SSLVPN SMA100 that an attacker could exploit to gain access to and modify a victim host's backend database, facilitating attacker access to administrator credentials which can be used to remotely execute arbitrary code on a victim's host.
- **CVE-2021-31206:** Accenture identified one actor selling and four financially motivated actors wanting to buy a CVE-2021-31206 exploit. CVE-2021-31206 is a data-processing error vulnerability (CWE-19) in Microsoft Exchange Server 2013-2019 an actor could exploit to enable the execution of arbitrary code on a victim's host.

Actors begin to capitalize on Log4j vulnerability

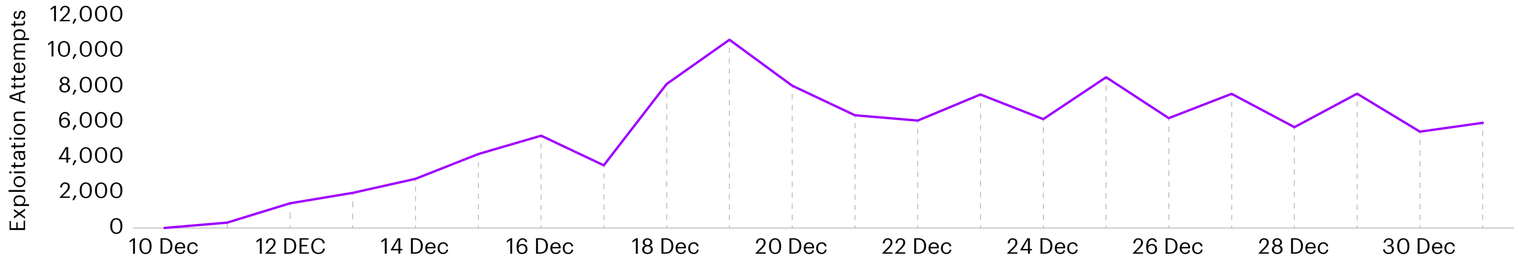
On December 9, 2021, Log4j maintainers reported details surrounding a remote code execution vulnerability,[22] identified as both CVE-2021-44228 and Log4Shell, that could allow attackers to execute arbitrary code on a vulnerable host. Successful exploitation would allow attackers to execute code without authentication. Because exploitation occurs by logging input, the attack surface for this vulnerability is extremely large. The first reported major exploitation occurred in a popular online video game. Another observed usage of the vulnerability involved a user changing their phone's device name and using that device name to inject code into the phone manufacturer's cloud service.

In late December 2021 there were first reports of a worm leveraging Log4j in the wild, more evidence of threat actors' interest in exploiting Log4j, and a new Log4j attack vector via WebSockets. CISA estimates there are 100 million affected software and technology instances across a wide range of technology products and vendors."

In December 2021, Accenture identified underground actors capitalizing on the news of the Log4j vulnerability. Threat actors began identifying ways to incorporate the vulnerability into attacking vulnerable companies and leveraging the access in botnet operations. In January 2022, actors began to research networks and IP addresses vulnerable to the Log4shell weakness and started selling their analysis to fellow underground actors.[23]

Figure 7. Log4j Exploitation Trends and Volume, December 2021

This timeline of telemetry data on log4j vulnerability exploitation attempts reveals malicious actor targeting trends by industry and region.



11,153
Unique Attacker Source IP

119,514
Unique Exploitation Attempts

26
Targeted Industries
Majority:
Manufacturing
Financial Services
Healthcare

6
Targeted Regions
Majority:
North America
Asia Pacific, Japan
Europe, Middle East, Africa

Source: Accenture Managed Extended Detection and Response Security Incidents Telemetry Data, December 9-31, 2021

Where next?

Here are some ways to handle vulnerability exploits:

- **Robustly defend network access:** The most efficient avenues an adversary may take to monetize corporate access is selling access to a victim's network or extorting a victim through ransomware, data disclosure threats, or both. Measures to help defend an organization's network include the implementation of zero trust principles, network security monitoring, such as deploying detection signatures to catch exploitation attempts against a specified environment and alerting on processes that execute from a specified system or web application log directory, strict access controls and endpoint controls. Block connections from the domains, IP addresses, and URLs, which have actively scanned and exploited known vulnerabilities. Block egress and recursive DNS on servers. Actors may attempt to leverage web and application servers to resolve calls to public websites holding malicious code. Also harden outbound firewall and WAF rules to block these types of calls from your environment.

- **Get back to security basics:** Often, organizations can prevent successful attacks by exercising regularly scheduled patch management programs, conducting an inventory of its environment's systems and software, and proactively testing existing technologies for weaknesses. Pairing patch management programs with cyber threat intelligence monitoring of the Dark Net marketplaces can provide context as well as inform defense postures as tactics when new vulnerabilities emerge such as Log4j in December 2021.

- **Update Log4j versions:** Log4j versions 2.0-beta9 to 2.14.1 are vulnerable to this vulnerability. To mitigate this vulnerability in those Log4j versions, Accenture suggests updating Log4j to version 2.17.0 for Java 8 (or later). Users should upgrade Log4j running on Java 7 to release 2.12.2. Apache, Accenture, and other cybersecurity outlets previously recommended using version 2.15.0 as a fix for this vulnerability; however, the fix was incomplete. Version 2.15.0 allowed code execution in certain configurations and neither Apache nor Accenture still consider it an official fix. The vulnerability caused by the incomplete fix in version 2.15.0 is CVE-2021-45046. On December 18, 2021, MITRE published CVE-2021-45105; this vulnerability affects Log4j versions 2.0-beta9 to 2.16.0. CVE-2021-45105 allows remote attackers to cause a denial of service via infinite recursion when the application encounters inputs with recursive lookups. Apache resolved this vulnerability in version 2.17.0.

  Apache has provided the official patch changelog here:

  https://logging.apache.org/log4j/2.x/security.html

  If it is not possible to update to version 2.17.0, users of Log4j versions 2.10 and later can mitigate this vulnerability by removing the JndiLookup class from the following class path:

  zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

  Longer term, organizations should inventory their environment's systems and software. Use application dependency mapping software to identify any software dependencies on the Log4j library. SCA tools like Veracode, Blackduck, and Sonatype, have plug-ins to identify this issue. Other vulnerability scanners like Qualys, Tenable, and Rapid7, have released plug-ins to detect this issue and administrators should update them regularly as long as this situation regarding CVE-2021-44228 exploitation continues to develop.

  As soon as possible, patch internal and Internet-facing software that use Log4j.[24]

References

1. Accenture Cyber Threat Intelligence, "Colonial Pipeline Ransomware," May 9 2021. IntelGraph reporting.
2. Accenture Cyber Threat Intelligence, "Ransomware Trends Q3 2021," November 11, 2021. IntelGraph Reporting; 2021 IBM Security X-Force Cloud Threat Landscape Report.
3. Accenture Cyber Investigations and Forensic Response research.
4. vx-underground Twitter post, October 28, 2021.
5. Accenture Cyber Threat Intelligence, "A View from the Dark Web: Are Ransomware Gangs Shifting Their Focus towards Europe?" November 15, 2021. IntelGraph reporting.
6. @darktracer Twitter account, November 17, 2021
7. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor." Mandiant. December 13, 2020.
8. "Two NPM Packages With 22 Million Weekly Downloads Found Backdoored," The Hacker News. November 7, 2021. "Newly Found npm Malware Mines Cryptocurrency on Windows, Linux, macOS Devices," October 20, 2021. "The inside story of ransomware repeatedly masquerading as a popular JS library for Roblox gamers," November 16, 2021.
9. Ibid.
10. "APT trends report Q3 2021," Kaspersky, October 26, 2021.
11. "TeleBots are back: Supply-chain attacks against Ukraine," ESET. June 30, 2017.
12. Accenture "Application Security"
13. "SUNSPOT: An Implant in the Build Process," CrowdStrike, January 11, 2021.
14. "Japanese government official says Olympic ticket data leaked," ZDNet, July 21, 2021.
15. Accenture Cyber Threat Intelligence, "Technical Analysis of REDLINE Stealer," April 19, 2021. IntelGraph Reporting.
16. "Hackers leak full EA data after failed extortion attempt," The Record, July 31, 2021.
17. Aggarwal, Gaurav, "How the pandemic has accelerated cloud adoption," Forbes, January 15, 2021.
18. Gartner® Press Release, Gartner says Four Trends are Shaping the Future of Public Cloud, August 2, 2021. GARTNER is the registered trademark and service mark of Gartner Inc., and/or its affiliates in the U.S. and internationally and has been used herein with permission. All rights reserved.
19. vx-underground Twitter post, October 28, 2021.
20. Accenture Cyber Threat Intelligence, "TeamTNT Operations Show the Cloud Is the New Battleground", January 14, 2022, Intelgraph reporting.
21. "TeamTNT with new campaign aka 'Chimaera'," AT&T. September 8, 2021.
22. Accenture Cyber Threat Intelligence, "Log4j Unauthenticated RCE CVE-2021-44228 Vulnerability," January 4, 2022, Intelgraph reporting.
23. Accenture Cyber Threat Intelligence, "Account "leopoldo787" Advertises List of 500,000 IP Addresses Potentially Vulnerable to Log4j Exploitation," January 2, 2022, IntelGraph reporting.
24. Accenture Cyber Threat Intelligence, "Log4j Unauthenticated RCE CVE-2021-44228 Vulnerability," January 4, 2022, Intelgraph reporting.

Contacts

Joshua Ray
Managing Director
Accenture Security
joshua.a.ray@accenture.com

Howard Marshall
Managing Director
Accenture Security
howard.marshall@accenture.com

Robert Boyce
Managing Director
Accenture Security
Global Cyber Investigations,
Forensics & Response (CIFR) Lead
r.boyce@accenture.com

Christopher Foster
Senior Principal – Security Innovation
Accenture Cyber Threat Intelligence
Product Strategy Lead
c.foster@accenture.com

Valentino De Sousa
Senior Principal – Security Innovation
Europe and Latin America
Cyber Threat Intelligence Lead
valentino.de.sousa@accenture.com

Contributors

Omar Al-Shahery, Gian Luca Giuliani,
Randall R. Griffith, Paul Mansfield,
Hannaire Mekaouar, Nellie Ohr,
Max Smith, Thomas Willkan
and the Cyber Investigations,
Forensics & Response (CIFR) team.

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 674,000 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 **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**, **LinkedIn** or visit us at **accenture.com/security**.

210863