Security threat intelligence report

Top 10 cyber threats of 2021

Konni RAT variant malware emerges

AdLoad campaign evades Apple malware scan

Potential threats to undersea cables surface

Atlassian patches critical code execution vulnerability in Confluence

October 2021
Message from Mark Hughes

Cyber threats continue to evolve and proliferate at increasing speed. Opportunistic attackers are taking advantage of everything from remote working and cloud configuration errors to poorly defended operational technology protecting vital infrastructures. And they’re becoming more professional with models like ransomware as a service. In honor of Cybersecurity Awareness Month, this issue looks at the top 10 threats of 2021 and the ways organizations can protect against them. Because the best defense is always good cyber hygiene, we review the basics that organizations should be sure to get right.

Mark Hughes
President of Security
DXC Technology

About this report

Fusing a range of public and proprietary information feeds, including DXC’s global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

Intelligence cutoff date:
September 28, 2021
Threat updates

Top 10 cyber threats of 2021 and how to guard against them

Cyber Security Awareness is once again in focus during the month of October. 2021 has shown nearly every industry that cyber threats are more sophisticated and pervasive than ever before. DXC Technology has identified 10 major threat types that are presenting major challenges to organizations worldwide in 2021. We've also outlined our top strategies for defending against these threats.

1. **Supply chain threats.** Supply chain attacks such as Solar Winds are expected to quadruple in 2021 over last year. These attacks are particularly problematic because even if your own security is robust, they can infiltrate your environment through vulnerabilities in your suppliers' security.

2. **Attacks on Linux and other non-Microsoft operating systems.** Attackers are increasingly expanding beyond the Microsoft operating system. For example, Vermilion Strike rewrote the Cobalt Strike Windows red team tool to attack Linux systems.

3. **Persistence of major ransomware players.** Major ransomware gangs such as the REvil ransomware-as-a-service operation do not generally disappear, but rather hibernate to avoid increased scrutiny or reform under new names. The ransomware-as-a-service model has enabled these groups to greatly expand their affiliate hackers and revenues.

4. **Remote work force vulnerabilities.** In a recent survey, 67 percent of respondents said attacks had targeted remote workers and 74 percent said an attack had resulted from vulnerabilities related to COVID-19. It appears companies have not sufficiently adapted their security strategies in response to the new remote workforce reality.

5. **Cloud attacks due to misconfiguration.** According to IBM, two-thirds of recent cloud breaches “would likely have been prevented by more robust hardening of systems, such as properly implementing security policies and patching systems.” Issues with credentials and policies “trickled down to the most frequently observed initial infection vectors (including) improperly configured assets, password spraying, and pivoting from on-premises infrastructure.”

6. **Zero-day threats.** New security vulnerabilities not matching any known malware signature have reached new highs in 2021, with at least 66 zero-day viruses and other malware found in use already this year.

7. **Threats to operational technology (OT) systems.** Attacks on OT devices – such as the Colonial Pipeline compromise – skyrocketed 46 percent in 2021. Utilities and manufacturing sectors are particularly at risk. Cyber security measures for OT are still weak or nonexistent in many cases.
8. **Brand abuse attacks.** In almost half of the fraud attacks through Q2 2021, cybercriminals impersonated credible brands to harvest consumer login credential or personal data. These attackers spoofed digital content and experiences by creating fake social media profiles, rogue mobile apps or hoax websites.

9. **Ransomware recovery key destruction.** Some ransomware gangs such as Grief and Ragnar Locker have threatened to delete victims' decryption keys if an organization involves authorities or a negotiation firm, rendering data unrecoverable.

10. **Zero-click mobile threats.** These insidious attacks, which enable malware to install itself on a victim’s device without the person clicking on a link, are on the rise for Android and Apple devices.

**The best defense: good cyber hygiene**

In DXC’s experience, the best defense against sophisticated emerging threats is to get the basics right. Simple mistakes such as misconfigured cloud settings, weak passwords, and unpatched or outdated software can lead to major operational disruption and data leaks.

Follow these fundamental security hygiene practices to ensure you’re well-fortified against both known and emerging threats:

- **Get configurations right.** Review your configuration management database (CMDB) and plan a decision process that defines security tiers from most to least secure.

- **Monitor the security controls that you set up.** If an alert is triggered but no one notices it quickly, the hackers will have time to gain a foothold in your environment.

- **Improve identity management.** Problems often result from having too many highly privileged accounts, especially if some are disabled or unused, or from a lack of multifactor authentication.

- **Know your crown jewels.** Determine which assets are essential for the organization’s survival and which are less critical, then assign security controls accordingly.

- **Increase visibility into third-party suppliers.** Identify, document and define the risks associated with all your third-party suppliers and service providers.

- **Keep up with patching and updating.** Establish good coordination between the IT department and the security organization so you can verify that software and operating systems patching directives are carried out across the entire organization by operational IT teams.

- **Keep and secure reliable backups.** Perform regular, complete backups for all essential systems and isolate them to protect from attacks. Know how to rebuild quickly from the backup and perform disaster recovery exercises regularly.

---

Former U.S. intelligence operatives charged with helping UAE hack rivals

The Justice Department charged three former intelligence operatives with hacking and conspiracy charges in connection with their work helping United Arab Emirates spy on activists and political rivals. The charges allege that defendants “knowingly and willfully” provided the UAE with spy technology without approval from the U.S. government. The charges back up a 2019 Reuters investigation that found a secret hacking unit of UAE-based security firm DarkMatter was hiring former U.S. intelligence officers to help the UAE to spy on the phones of activists, diplomats and other national leaders.

Source: CyberScoop
• **Build security into all new applications and solutions.** Security should not be a second thought; it’s more effective and ultimately simpler to build it in from the start, using native capabilities of your cloud platforms and operating systems when possible. Validate security once new systems go live with penetration testing and vulnerability scanning.

**Sources**
- ENISA
- Tenable/Forrester
- IBM
- MIT Technology Review
- Skybox
- Outseer

**Konni RAT variant malware emerges**

Konni RAT malware campaign deploys new variant.

**Targets Russia**

KONNI, a Windows remote access Trojan (RAT) that has been in use since 2014, has a new more pervasive variant that has been observed targeting victims in Russia. KONNI, which has similar code attributes with the NOKKI malware family, has been linked to several campaigns involving North Korean themes.

Malwarebytes researchers observed a spear-phishing campaign deploying Konni RAT spread by malicious emails that contained one of two documents written in Russian and related to trade and economic issues between Russia and the Korean peninsula.

Both documents were weaponized with the same malicious macro and contain malware that uses two different techniques to bypass the User Account Control (UAC), a security feature that helps prevent unauthorized changes to Windows 10 PCs or devices. This new variant applies obfuscation techniques to avoid detection.

The following is tailored to SOC/hunt teams, focusing on TTPs and IOCs to assist the workflow of those teams, though it is not intended to be a full malware analysis of Konni RAT.

**Konni RAT install process:**

Users receive an email with a Microsoft Word doc attached, open the document and enable content/macro. Once enabled, the macro initiates the following series of activities to deploy the Konni RAT.

95%

volume of intercontinental Internet traffic carried over undersea cables and vulnerable to attack

Source: Atlantic Council

15%

share of 2020 ransomware payments that carried risk of government sanctions

Source: CyberScoop
Wscript Shell function executes the Java Script file:

• y.js

The Java Script file y.js drops and executes the following two files:

• yy.js - a second Java Script file
• y.ps1 - a Powerscript file

Note: Wscript shell is used again to execute the files.

The Powershell script y.ps1 will configure system to download a Cabinet (CAB) file.

• The file is downloaded from: takemetoyouheart[.]c1[.]biz/index[.]php?user_id=319
• The CAB file is stored at: %APPDATA%Temp directory
• The file name is unique random name created by GetTempFileName.
• WinExec will execute a cmd command to extract data from the CAB file and delete it.
• y.ps1 will also be deleted. Note: This may not be a huntable IOC.

The extracted cabinet file contains five files:

• check.bat
• install.bat,
• xmlprov.dll
• xmlprov.ini
• xwtpui.dll

The yy.js Java Script file:

• Executes the check.bat file.
• yy.js then deletes itself.

Note: This may not be a huntable IOC.

check.bat file:

• The check.bat file batch checks if the command prompt is launched as administrator using net session > nul.
• If Command Prompt is admin level, install.bat file executes.
• If the the Command Prompt is not launched with elevated privileges:
  • check.bat checks the OS version
  • If Windows 10 sets a variable named num to 4, otherwise it sets it to 1.
It then executes xwtpui.dll using rundll32.exe by passing three parameters to it:

- **EntryPoint** (The export function of the DLL to be executed),
- **num** (the number that indicated the OS version)
- **install.bat

**install.bat file:**

- The malware used by the attacker pretends to be the xmlprov Network Provisioning Service.
- This service manages XML configuration files on a domain basis for automatic network provisioning.
- **install.bat** is responsible to install xmlprov.dll as a service.

**Installation process for xmlprov.dll:**

- Stop the xmlprov service
- Copy dropped xmlprov.dll and xmlrov.ini into the system32 directory and delete them from the current directory. Note: This is a detection opportunity.
- Add xmlProv to the list of the services to be loaded by svchost.
- Add xmlProv to the xmlProv registry key. Note: Detection opportunity.
- Start the xmlProv service

**UAC bypass techniques:**

**Calvary UAC Bypass**

- Calvary is a token impersonation/theft privilege escalation technique that impersonates the token of the Windows Update Standalone Installer process (wusa.exe). Note: wusa.exe is often alerted on by EDR tooling. FP rate is high.
- wusa.exe will spawn cmd.exe with highest privilege to execute install.bat.
- Note: This offers only limited detection opportunities.

**Windows 10 UAC Bypass**

- The UAC bypass used for Windows 10 uses a combination of a modified version of RPC-based UAC bypass reported by Google project Zero and Parent PID spoofing to bypass UAC.

Google Link: hxxps://googleprojectzero.blogspot.com/2019/12/

- Note: There are other steps to this process, none of which produce any detection or hunt opportunities and are outside the scope of this report.

**Xmlprov.dll (Konni RAT)**

- Konni RAT payload is deployed as a service using svchost.exe.

---

46%

Increase in attacks against OT devices in 2021

Source: Outseer

150

number of unique samples in AdLoad's new Trojan-based campaign, some of which were approved by Apple's notarization service

Source: Intego
Konni Rat is heavily obfuscated and is using multiple anti-analysis techniques.

- It has a custom section named “qwdfr0,” which performs all of the de-obfuscation processes.
- The payload registers itself as a service using its export function, ServiceMain.

Konni RAT starts by collecting information from the target machine by executing several commands.

**cmd /c systeminfo**

- Uses this command to collect the detailed configuration information about the target machine including:
  - Operation system configurations
  - Security information
  - Hardware data (RAM size, disk space and network cards info)
- Config data is stored in a tmp file

**cmd /c tasklist**

Executes this command to collect a list of running processes on victims’ machine and store them in a tmp file. Each of the collected tmp files is converted into a cab file:

- Command used: cmd /c makecab (detection opportunity)
- Files are encrypted and sent to the attack server in an HTTP POST request

http://taketodjnfnei898.c1.biz/up.php?name=%UserName% (detection opportunity)

After sending data to the C2, it goes to a loop to receive commands from the server:

- http://taketodjnfnei898.c1.biz/dn.php?name=%UserName%&prefix=tt (detection opportunity)

Malware process flow diagram provided by Malwarebytes Labs:

---

Azure Active Directory password brute-forcing flaw has no fix

Researchers at Secureworks Counter Threat Unit in June discovered a flaw in the protocol used by Azure Active Directory Seamless Single Sign-On service. This flaw allows threat actors to perform single-factor, brute-force attacks against Azure Active Directory without generating sign-in events in the targeted organization’s tenant.

Source: Ars Technica
JavaScript files have been used to execute batch and PowerShell files. In each of the campaigns, threat actors used macro weaponized documents to download a cab file and deploy the Konni RAT as a service.

Note: A CAB file is a Windows cabinet file saved in an archive format native to Microsoft Windows. Typically, CAB files contain Windows system or device driver updates. The CAB format supports the .ZIP, Quantum and LZX data compression algorithms. CAB files contain compressed data and are used for Windows software installations, such as system files, network components and device drivers.

Files are encrypted and sent to the attack server in an HTTP POST request:

• hxxp://taketodjnfnei898.c1.biz/up.php?name=%UserName% (detection opportunity)

After sending data to the C2, it goes to a loop to receive commands from the server:

• hxxp://taketodjnfnei898.c1.biz/dn.php?name=%UserName%&prefix=tt (detection opportunity)

The VirusTotal detection is a Low AV detection rate.

Impact

KONNI RAT has the ability to gather information to profile an IT environment for networked computer systems through host enumeration, keystroke logging and screen captures. Information collected can then be used to craft specific attacks based on the information that was obtained.

DXC perspective

All of the basic features for a backdoor are present, including host profiling and remote access and control. The new KONNI RAT variant is more sophisticated than the original in its ability to remain undetected, which could pose a significant threat to targets outside of Russia. DXC will continue to monitor for new details as additional information becomes available.

Sources:

Malwarebytes Labs
FileInfo
Mitre ATT&CK
CISA

BlackMatter ransomware hits food cooperative

Iowa-based New Cooperative publicly disclosed that it had been hit by the Russia-tied BlackMatter cyber cell in an attack that locked up its computers used to manage food supply chains and animal feeding schedules. BlackMatter, directly related to the notorious DarkSide crew that carried out the Colonial Pipeline operation in early 2021, has threatened to publish a terabyte of data it claimed to have stolen from the co-op, which reportedly has refused to pay the $5.9 million ransom demand. BlackMatter breached hundreds of employee credentials left exposed by poor password management. Researchers found the “chicken1” password was used more than 10 times among the company’s 120 employees. Passwords used by some of the co-op’s top executives also were compromised. To date 653 instances of breached credentials are connected to New Cooperative.

Source: MSS Alert
AdLoad campaign evades Apple malware scan

A new variant of the AdLoad campaign launched in August has been shown to evade Apple XProtect, the manufacturer's on-device malware scanner.

AdLoad is an adware infection that installs a man-in-the-middle web proxy that redirect the user's web traffic through the attacker's own preferred servers, with the goal of hijacking and redirecting web browsers for monetary gain.

The new campaign is comprised of 150 unique samples, and select samples were approved by Apple's notarization service, a process whereby all third-party software distributed outside of the Mac App Store must be uploaded to Apple's servers and checked for malware. If the software passes Apple's malware scan check, its details are added to Apple's database of "safe" or at least "allowed" software. Developers in return receive an electronic ticket that can be attached to the software by the developer when distributing it.

AdLoad 2021 campaign TTPs and IOCs

Attack Vector:

- This variant of AdLoad is deployed via an OSX/Bundlore Trojan horse.
- The Trojan masquerades as an Adobe Flash Player installer.
- Flash Player disguise is used during the installation process.
- The user is asked to install and/or update Flash.
- The Trojan in this campaign sample is a malicious link that redirects to a malicious Video Player app download (Player.app), which is mounted in a DMG.
2021 variants of AdLoad used persistence and executable names that followed a consistent pattern and uses the following file extensions:

```
.system
.service
```

The file extension used varies on the location of the dropped persistence file and executable. Both the .system and .service files can be found on the same infected device if the user gives privileges to the installer.

Despite privilege level - AdLoad will install a persistence agent in the user’s Library LaunchAgents folder.

**LaunchAgents folder pattern examples:**

- `~/Library/LaunchAgents/com.ActivityInput.service`
- `~/Library/LaunchAgents/com.AnalyzerWindow.service`
- `~/Library/LaunchAgents/com.AssistiveFile.service`
- `~/Library/LaunchAgents/com.BoostConsole.service`
- `~/Library/LaunchAgents/com.DefaultTool.service`
- `~/Library/LaunchAgents/com.ElementaryType.service`
- `~/Library/LaunchAgents/com.ExtendedSprint.service`
- `~/Library/LaunchAgents/com.SwitcherGuard.service`

Droppers observed were an obfuscated Zsh script (Zsh obfuscation is used because it is not well-recognized by static signature scanners on VirusTotal).

The malware executes out of the /tmp directory. See the following screen captures:

![Screen capture](image1.png)

**Executable Paths:**

- `~/Library/Application\ Support/[0-9]{19}/Services/com.<label>.service/<label>.service`
- `~/Library/Application\ Support/[0-9]{19}/System/com.<label>.system/<label>.system`
Dropper Hashes:
• 8bf1defb2feaa1880f0f9b98e863276dc4cb7a3e5
• 9912549c3a86e222a5684a3c04d76bdfda4c
• 400138e08e0fca1220e1982f24dd1b20868d

DMG Hashes and Details:
MD5: 45aed46565694d868eb7932af04e4e1e
SHA-1: 8bf1defb2feaa1880f0f9b98e863276dc4cb7a3e5
SHA-256: 1724942eeec7c367238409d06d6c93a3477998c124a2a9f6f78c425533af17
SSDEEP: 24576:kragxJVU32JNvzxQfjbyC08s19DAOWy28xsasvPGwRTo8d65rW/ErPczNH9wPq2:kC3QoR1xs1pealGwC75RrPc19wPHkQv
File type: Macintosh Disk Image
File size: 1.45 MB (1518608 bytes)
Name: Install.dmg

Flash Player Hashes and Details:
File Name: flashplayerinstaller.dmg
• ef00a38c2ccc662b0fe7f9b6895ce2da593f72870c25b9b0cb3e267f757511e7
• a0edadd6620ef0171180b20b6925b3f25b9d1755b14201375c3d0e3cf8fac0
• c9e50c165421bacb73c597f475ccc5f4fd2169a75b205d81c2f5b9493a2292d0

Impact
AdLoad can escalate privileges to root by asking the user for credentials and can use bash scripts to check the macOS version and download payloads, with the goal of redirecting user's web browsers. Targeted industries include all Mac users, media and education sectors as well as any organizations that use Apple products within their environment.

DXC perspective
The fact that Apple's XProtect is not effective in prohibiting the malware from installing on users' Mac devices is a concern. Third-party antivirus products do recognize the malicious activity but appear to be ineffective at detecting AdLoad. Organizations are advised to alert Mac users to phishing efforts that involve Flash player installation and hunt for IOCs on potentially affected machines.

Sources:
VTI Security
Intego
Malpedia
Vulnerability Updates

Atlassian patches critical code execution vulnerability in Confluence

Atlassian informed customers regarding the availability of patches for a critical vulnerability affecting the company’s Confluence enterprise collaboration product. Atlassian described the flaw as an OGNL injection issue that can be exploited by an authenticated attacker — and in some cases an unauthenticated attacker — to execute arbitrary code on affected Confluence Server and Data Center instances.

Impact

The vulnerability, tracked as CVE-2021-26084 with a CVSS score of 9.8, has been fixed with the release of versions 6.13.23, 7.4.11, 7.11.6, 7.12.5 and 7.13.0.

DXC perspective

Please refer to the Confluence Security Advisory for resolution methods and workarounds.

Source:
Atlassian
Nation State and Geopolitical

Potential threats to undersea cables surface

The U.S. government, its allies and any other organizations may have to work together to form an alliance to address the security and resilience of undersea cables, which carry Internet traffic around the world.

Beijing and Moscow are stepping up their efforts to buy or influence companies responsible for laying the undersea cables that shuttle online communications between countries and servers. The Atlantic Council fears that undersea cable companies either owned or influenced by Beijing and Moscow could be forced to compromise security by inserting backdoors or allowing intelligence agencies to monitor landing stations in order to intercept traffic.

The council, a nonpartisan organization that galvanizes U.S. leadership and worldwide engagement in collaboration with allies and partners, warns: “It is estimated that upwards of 95 percent of intercontinental Internet traffic is carried over these cables. Without them, the Internet would not exist as it does today. These cables are largely owned by private companies, often in partnership with one another, though some firms involved in cable management are state-controlled or intergovernmental. Submarine cables are, therefore, a major vector of influence that companies have on the global Internet’s shape, behavior and security.”

Source:

Atlantic Council
DXC in security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers. DXC provides solutions tailored to our customers’ diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Risk Management. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit dxc.com/security.

Stay current on the latest threats
dxc.com/threats

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world’s largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at dxc.com.