Cyber Intelligence Brief

Aug 07 - 13, 2021

See Threats. Stop Breaches. Together

Prepared by ***deepwatch Threat Intelligence Team***

Denver Office & SOC

7800 East Union Avenue, Suite 900

Denver, CO 80237 USA

855.303.3033

Purpose

This report is provided to you to improve your situational awareness and educate recipients of cyber events to aid in protecting organizations' networks, proprietary and personally identifiable information from unauthorized access, theft, or espionage. In addition, deepwatch includes additional insights and recommendations and any actions we may have taken if applicable.

Sources of Information

This publication incorporates open-source news articles to educate readers on cybersecurity matters IAW USC Title 17, section 107, Para a. All articles have been truncated to avoid the appearance of copyright infringement.

Use and Definitions

To help you use this document to its full potential a few items may be helpful to know:

- You can click on any item in the table of contents to take you to that portion of the report.
- Links throughout this document are identified by the font color of "deepwatch" Green.
- Your feedback will be extremely valuable to the deepwatch Threat Intelligence Team; please take a few minutes to send us your feedback here. Your feedback submission can be anonymous. We read each submission carefully. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.
- Each headline will be categorized; these categories quickly let you know what the main topic of the headline is.
- Each headline this report covers includes the following information:
    - A headline, publication date, and a link to the source material.
    - A section that includes Activity Groups identified, Impacted Industries, and Region.
    - Summary - This is a brief synopsis of the reporting to bring you only the most relevant information. If applicable, deepwatch will link items of interest for further context; these will be in "deepwatch" Green.
    - deepwatch Insights - This section may include additional analysis and reporting on the activity if applicable, any recommendations, and any actions deepwatch may have taken with the available information.
- If MITRE ATT&CK tactics and techniques are identified, these will be listed in Appendix A and associated deepwatch detections.
- If IOCs are identified, these will be listed in Appendix B.

Table of Contents

Quick Look

Headline: Accenture Downplays Ransomware Attack as LockBit Gang Leaks Corporate Data | Data Leak

- **Key Takeaway**
  - Accenture confirmed it was a victim of a ransomware attack but stated: "*it had little impact on the company's operations.*" and that they "*fully restored our affected systems from back up.*" LockBit Ransomware operators claimed to have several Terabytes of internal data and posted them on their leak site.
- **deepwatch Response**
  - deepwatch employs numerous detection strategies to observe known ransomware operators' TTPs.

Headline: A Look Inside the Operations and Tradecraft of the Conti Ransomware Gang | Ransomware

- **Key Takeaway**
  - Fortinet analyzed a training manual titled "CobaltStrike Manuals_V2 Active Directory" that was recently part of a 113 MB leak by a disgruntled Conti affiliate. The manual instructs affiliates on the use of Cobalt Strike, Mimikatz, and other open-source tools.
- **deepwatch Response**
  - deepwatch employs numerous detection strategies to observe known ransomware operators' TTPs.

Headline: New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices | Ransomware

- **Key Takeaway**
  - A new variant of the eCh0raix ransomware has been detected, combining features to target both QNAP and Synology NAS devices. Threat actors are taking advantage of the vulnerability CVE-2021-28799 in QNAP devices to distribute this new variant. Once exploited, the vulnerability allows remote attackers to log in to the device.
- **deepwatch Response**
  - deepwatch recommends users of Synology and QNAP NAS devices update the firmware to prevent attacks of this nature. Details about updating QNAP NAS devices against CVE-2021-28799 can be found on the QNAP website. In addition, it is recommended that organizations implement a sound password policy that makes brute-forcing more difficult for attackers and configure SOHO-connected devices to only accept connections from a hard-coded list of recognized IPs to prevent network attacks.

Headline: Abusing Misconfigured Salesforce Communities for Recon and Data Theft | SaaS Security

- **Key Takeaway**
  - Varonis identified how a misconfigured "*Salesforce Community may lead to sensitive Salesforce data being exposed to anyone on the internet.*"
- **deepwatch Response**
  - deepwatch recommends following the recommendations provided by Varonis to secure your Salesforce Community platform

Headlines

Data Leak | Accenture Downplays Ransomware Attack as LockBit Gang Leaks Corporate Data

August 11, 2021
Source: *The Record by Recorded Future*

Key Points:

- Well-known consulting and Fortune 500 company Accenture confirmed they were a victim of a ransomware attack.
- LockBit Ransomware operators claimed to have several Terabytes of internal data and were posted to their leak site.
- Files that were leaked did not appear to contain sensitive information, according to the article.

Summary:

Global Fortune 500 company Accenture confirmed it was a victim of a ransomware attack but stated to ZDNet "it had little impact on the company's operations." And in an email statement provided by The Record said they "*fully restored our affected systems from back up.*"

In an emailed statement published in the article, Accenture stated:

> Through our security controls and protocols, we identified irregular activity in one of our environments. We immediately contained the matter and isolated the affected servers. We fully restored our affected systems from back up. There was no impact on Accenture's operations, or on our clients' systems.
>
> *Accenture spokesperson*

Around 1:30 PM EST, LockBit gang leaked Accenture's files, which, following a cursory review by The Record shows that they "*appeared to include brochures for Accenture products, employee training courses, and various marketing materials. No sensitive information appeared to be included in the leaked files.*"

deepwatch Insights
Ransomware operators routinely use the same Tactics, Techniques, and Procedures (TTPs) similar to a typical business-like workflow or process due to their human-operated intrusion and ransomware activities. Additionally, these TTPs are routinely observed by different Ransomware Variant Operators due to their highly successful outcomes. deepwatch employs numerous detection strategies to capture these known TTPs.

Back to Table of Contents

Ransomware | A Look Inside the Operations and Tradecraft of the Conti Ransomware Gang

August 10, 2021
Source: *Fortinet*

Key Points:

- A disgruntled affiliate of the Conti ransomware gang recently leaked a 113 MB file that contained numerous tools and training manuals.
- Fortinet analyzed one of the training manuals titled "CobaltStrike Manuals_V2 Active Directory."
- The manual instructs affiliates on the use of Cobalt Strike, Mimikatz, and other open-source tools.

Summary:

Fortinet analyzed the recent leak of the Conti ransomware gang's support manual, titled "CobaltStrike Manuals_V2 Active Directory." Their analysis highlights the operational procedures of the Conti ransomware group. Additionally, the manual provides affiliates instructions in the following areas:

- The usage of Cobalt Strike and steps the affiliate should take once a reverse shell or persistence is established with the victim's Windows Domain Controller.
- Suggests that affiliates conducting Kerberoast activities use the tool Invoke-Kerberoast.ps1.
- The manual provides a simple overview of Mimikatz and functional command lines to extract clear passwords from memory, Kerberos tickets, etc.
- The manual also guides affiliates on using the open-source tool SMBAutoBrute.
- The manual has instructions on the usage of Mimikatz via a Cobalt Strike beacon to dump hashed domain controller passwords via NTDS.dlt Once this is performed, the affiliate is instructed to install Anydesk on all abandoned hosts and Atera on the rest.
- The manual suggests affiliates use the tool RClone to automate the exfiltration.
- The manual provides several instructions for Linux, the various flags to look for to locate known and unknown drives, disabling VMware services, including ESXi, deleting shadow copies, and engaging in mass lock.

deepwatch Insights

Conti RaaS affiliates are instructed, and many have used remote connection platforms like AnyDesk, Atera, Splashtop, Remote Utilities, and Screen Connect to initialize and maintain persistent network access. Therefore deepwatch recommends that organizations block all remote access connections from these programs by utilizing application controls if there is no current business use case for them.

Fortinet recommends that organizations ensure that all known vendor vulnerabilities are addressed and updated to prevent attackers from gaining a foothold within a network. To accomplish this, deepwatch recommends conducting an assessment to prioritize risk and develop alternative risk reduction measures if patching is not feasible.

In addition to the measures listed above, deepwatch recommends incorporating a security awareness program within your organization to assist in training/educating users to identify different types of social engineering techniques used by many ransomware gangs.

Back to Table of Contents

Ransomware | New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices

August 10, 2021
Source: *Palo Alto Unit 42*

Key Points:

- A new variant of the eCh0raix ransomware has been detected, combining features to target both QNAP and Synology NAS devices.
- Threat actors are taking advantage of the vulnerability CVE-2021-28799 in QNAP devices to distribute the new variant.
- Once exploited, the vulnerability allows remote attackers to log in to the device.

Summary:

Palo Alto's Threat Intelligence team, Unit 42, discovered a new variant of eCh0raix ransomware targeting Synology and Quality Network Appliance Provider (QNAP) network-attached storage (NAS) devices. The threat actors distributing the ransomware are taking advantage of the vulnerability CVE-2021-28799 in QNAP devices. Once exploited, the vulnerability allows remote attackers to log in to the device. This new variant is the first time Unit 42 has seen it combining features to target both QNAP and Synology NAS devices.

Small Office/Home Office (SOHO) users are attractive to ransomware operators because they are a stepping stone to target more prominent organizations through supply chain attacks. Unfortunately, SOHO users are generally less prepared to block ransomware attacks than larger organizations because they typically do not employ dedicated IT or security professionals.

deepwatch Insights

deepwatch recommends users of Synology and QNAP NAS devices update the firmware to prevent attacks of this nature. Details about updating QNAP NAS devices against CVE-2021-28799 can be found on the QNAP website. In addition, it is recommended that organizations implement a sound password policy that makes brute-forcing more difficult for attackers and configure SOHO-connected devices to only accept connections from a hard-coded list of recognized IPs to prevent network attacks.

Back to Table of Contents

SaaS Security | Abusing Misconfigured Salesforce Communities for Recon and Data Theft

August 10, 2021
Source: *Varonis*

Key Points:

- Misconfigured software platforms can expose organizations to sensitive data exposures.
- Varonis identified how a misconfigured "*Salesforce Community may lead to sensitive Salesforce data being exposed to anyone on the internet.*"
- Varonis researchers discovered how "*a malicious actor could exploit this misconfiguration to perform recon for a spear-phishing campaign... steal sensitive information about the business, its operations, clients, and partners.*"

Summary:

Misconfigured software platforms can expose organizations to sensitive data exposures, and Varonis identified how a misconfigured "*Salesforce Community may lead to sensitive Salesforce data being exposed to anyone on the internet.*" And learned that "*Anonymous users can query objects that contain sensitive information such as customer lists, support cases, and employee email addresses.*"

Varonis researchers discovered how "*a malicious actor could exploit this misconfiguration to perform recon for a spear-phishing campaign. At worst, they could steal sensitive information about the business, its operations, clients, and partners. In some cases, a sophisticated attacker may be able to move laterally and retrieve information from other services that are integrated with the Salesforce account.*"

deepwatch Insights

deepwatch agrees with following the recommendations provided by Varonis to secure your Salesforce Community platform:

- Adhere to the principle of least privilege and ensure that guest profiles only allow the minimum required permissions. Varonis has provided a step-by-step process available here.
- Ensure that API is enabled is unchecked. It's recommended to disable Access Activities as well. Varonis has provided a step-by-step process available here.
- Set a default owner for records created by guest users. Varonis's step-by-step process can be found here.
- Enable secure guest user record access. View Varonis's step-by-step process here.

Back to Table of Contents

Appendix A

Attack Vectors Featured This Week

Attack Vector Mapping Matrix		
Source	**MITRE ATT&CK Vector**	**deepwatch Detection**
A Look Inside the Operations and Tradecraft of the Conti Ransomware Gang	Masquerading T1036	dwa_auda_00011: Windows File Added/Modified
	Steal or Forge Kerberos Tickets: Kerberoasting T1558.003	dwa_auta_00014: Possible Kerberoasting (Multiple SPN Requested)
	Brute Force T1110	deepwatch has numerous detections to observe brute force activity
	Network Service Scanning T1046	dwa_enda_00024: Host Enumeration Command Execution dwa_idsa_00001: Internal Vulnerability Sweep Detection dwa_neta_00001: Internal Network Service Discovery dwa_neta_00008: Suspicious Port Scanning Activity vtsec_nwa1_00001: Suspicious Port Scanning Activity
	Automated Exfiltration T1020	dwa_inta_00030: File Transfer to Threat Host dwa_inta_00037: File Transfer to Threat Host dwa_neta_00002: File Transfer from Critical Host dwa_neta_00007: Executive System Exfiltration

Back to Table of Contents

Appendix B

IOCs Featured This Week

Hashes		
Source	**File Name**	**IOC**
Arcadyan Firmware Vulnerability CVE-2021-20090 Under Attack Exploitation	lolol.sh	**SHA256:** 9793ac5afd1be5ec55476d2c205260d1b7af6db7cc29a9dc0f7fbee68a177c78
	dark.arm5	73edf8bfbbeaccdd84204f24402dcf488c3533be2682724e5906396b9237411d
	dark.mips	8bb454cd942ce6680f083edf88ffa31661a47a45eb3681e1b36dd05043315399
	dark.m68k	f83eadaa00e81ad51e3ab479b900b981346895b99d045a6b6f77491c3132b58c
	dark.sh4	e4bc34e321b31926fd2fa1696136187b13864dfa03fba6848e59f9f72bfa9529
	dark.arm6	80331cf89f3e6026b33b8f1bfa1c304295b9327311661d7927f78824f04cf528
	dark.mpsl	904f9b2e029595365f4f4426069b274810510908c7dd23a3791a831f51e9f1fc
	dark.x86	283f932f30756408a59dac97a6965eb792915242214d590eab1c6cb049148582
	dark.arm7	c2f5bbf35afc7335f789e420c23c43a069ecfcca1a8f9fac5cd554a7a769440e
	dark.ppc	70764ef9800c1d09f965fbb9698d0eda52448b23772d118f2f2c4ba37b59fc20

IP Addresses	
Source	**IOC**
Arcadyan Firmware Vulnerability CVE-2021-20090 Under Attack Exploitation	27.22.80[.]19 212.192.241[.]72

Back to Table of Contents

Feedback

Please take a few minutes to send us your feedback here. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the deepwatch Threat Intelligence Team. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.

Back to Table of Contents