Cyber Intelligence Brief

August 14 - 20, 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 and/or IOCs are listed, these will be listed in the accompanying Appendixes.

Table of Contents

Quick Look

Headline: CISA Provides Recommendations for Protecting Information from Ransomware-Caused Data Breaches | Ransomware

---

- **Key Takeaway**
  - CISA released the fact sheet titled "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches". This fact sheet is a **MUST READ** for organizations wanting to learn how to protect themselves from ransomware attacks.
- **deepwatch Outlook**
  - Ransomware attack trends have only increased and it is highly recommended that organizations review and apply as many CISA guidelines as possible listed in the fact sheet. deepwatch recommends coordinating with your Squad Manager for further assistance on implementing the guidelines in the fact sheet.

Headline: Memorial Health System Confirms Cyber Attack | Ransomware

---

- **Key Takeaway**
  - Memorial Health System confirmed it was a victim of a cyberattack. Hive ransomware group is suspected to be behind the attack. Evidence has been seen that "*the attackers have stolen information belonging to 200,000 patients, which includes sensitive details.*"
- **deepwatch Outlook**
  - Ransomware groups will continue to exfiltrate sensitive data as another extortion method to coerce the victim organization to pay the ransom demand due to its high success rate. deepwatch Threat Intelligence Team routinely monitors the Ransomware operator space to drive deepwatch's numerous detection strategies to capture these known TTPs.

Headline: New HolesWarm botnet targets Windows and Linux servers | BotNet

---

- **Key Takeaway**
  - A new cryptomining botnet, HolesWarm, has been discovered. The malware exploits more than 20 known vulnerabilities to infiltrate Windows and Linux servers. At this time the botnet has primarily focused on China but it is expected to spread globally as its infrastructure and capabilities improve.
- **deepwatch Outlook**
  - The installation of cryptomining bots will continue as cryptocurrencies maintain or increase in value. deepwatch employs numerous detections to observe malicious file executions as well as known delivery and initial access infection vectors. deepwatch recommends determining the applicability of the IOCs listed in Appendix A and if necessary adding them to your blocklist.

Headline: Malware Campaign Uses Clever 'Captcha' to Bypass Browser Warning | Malware

---

- **Key Takeaway**
  - Threat actors are employing a clever technique to trick users by using a fake reCaptcha that allows the Banking Trojan (Gozi/Ursnif) malware to be downloaded and executed.
- **deepwatch Outlook**
  - deepwatch recommends warning end-users about this potential threat. In addition, deepwatch employs numerous detections to observe malicious file executions as well as known delivery and initial access infection vectors. deepwatch recommends determining the applicability of the IOCs listed in Appendix A and if necessary adding them to your blocklist.

Headlines

Ransomware | CISA Provides Recommendations for Protecting Information from Ransomware-Caused Data Breaches

August 18, 2021
Source: *US-CERT CISA (PDF)*

Key Points:

- CISA released the fact sheet titled "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches"
- CISA released the fact sheet *"to address the increase in malicious cyber actors using ransomware to exfiltrate data and then threatening to sell or leak the exfiltrated data if the victim does not pay the ransom."*
- The fact sheet provides *"information for organizations to use in preventing and responding to ransomware-caused data breaches."*

Summary:
CISA has released the fact sheet titled "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches." CISA released the fact sheet *"to address the increase in malicious cyber actors using ransomware to exfiltrate data and then threatening to sell or leak the exfiltrated data if the victim does not pay the ransom."* The goal of this fact sheet is to provide *"information for organizations to use in preventing and responding to ransomware-caused data breaches."*

CISA "*encourages organizations to adopt a heightened state of awareness and implement the recommendations listed in this fact sheet to reduce their risk to ransomware and protect sensitive and personal information. Review StopRansomware.gov for additional ransomware resources.*"

dw Threat Intelligence Outlook

Ransomware operators routinely share the same Tactics, Techniques, and Procedures (TTPs) and abandoned TTPs that are less successful. Ransomware operations will only increase and that is why it is imperative that organizations follow the guidelines as laid out in the fact sheet. deepwatch Threat Intelligence Team routinely monitors the Ransomware operator space to drive deepwatch's numerous detection strategies to capture these known TTPs. deepwatch recommends coordinating with your Squad Manager for further assistance on implementing the guidelines in the fact sheet.

Back to Table of Contents

Ransomware | Memorial Health System Confirms Cyber Attack

August 16, 2021
Source: *Bleeping Computer*

Key Points:

- Memorial Health System confirmed it experienced an attack that occurred in the early morning of Sunday, August 15th.
- Ransomware group Hive is suspected to be behind the attack.
- BleepingComputer has seen evidence that *"the attackers have stolen information belonging to 200,000 patients, which includes sensitive details, such as social security numbers, names, and dates of birth."*

Summary:
Memorial Health System, a small network of three hospitals in Ohio and West Virginia, confirmed it was a victim of a cyberattack that occurred in the early morning of Sunday, August 15th. The IT responded by suspending user access to IT applications related to their operations.

Memorial Health System released a statement on August 15th that stated *"Maintaining the safety and security of our patients and their care is our top priority and we are doing everything possible to minimize disruption," says Memorial Health System president and CEO Scott Cantley, "Staff at our hospitals- Marietta Memorial, Selby, and Sistersville General Hospital - are working with paper charts while systems are restored, and data recovered."*

The release also stated *"At this time no known patient or employee personal or financial information has been compromised," he said. "We are continuing to work with IT security experts to methodically investigate to precisely understand what happened and are taking the appropriate actions to resolve any and all issues."*

But BleepingComputer has seen evidence that the ransomware group Hive *"have stolen databases with information belonging to 200,000 patients, which includes sensitive details, such as social security numbers, names, and dates of birth."*

dw Threat Intelligence Outlook

The same Tactics, Techniques, and Procedures (TTPs) are routinely seen by ransomware groups as one group will incorporate the "best" features and tactics used by others as seen by the comments made by the new group BlackMatter. Ransomware groups will continue to exfiltrate sensitive data as another extortion method to coerce the victim organization to pay the ransom demand due to its high success rate. deepwatch Threat Intelligence Team routinely monitors the Ransomware operator space to drive deepwatch's numerous detection strategies to capture these known TTPs.

Back to Table of Contents

BotNet | New HolesWarm Botnet Targets Windows and Linux Servers

August 16, 2021
Source: *The Record by Recorded Future*

Key Points:

- A new cryptomining botnet named HolesWarm has been discovered.
- The malware has been exploiting more than 20 known vulnerabilities to infiltrate Windows and Linux servers.
- At this time the botnet has primarily focused on China but it is expected to spread globally as its infrastructure and capabilities improve.

Summary:

Tencent and other bloggers have discovered a new botnet named HolesWarm that has been slowly gaining since June this year. The new malware has been exploiting more than 20 known vulnerabilities to infiltrate Windows and Linux servers and then deploy cryptocurrency-mining malware.

The attacks have primarily focused on China but analysis of the botnet shows that it is expected to expand and target systems across the globe as its infrastructure and attack capabilities are expected to expand in the coming months.

Tencent Security says that once the malware is executed on a system, it will dump local passwords, traverse to the local network, and then deploy a cryptocurrency mining tool to mine Monero.

HolesWarm often leads to discovery because it maxes out the server CPUs instead of tethering the cryptomining process.

dw Threat Intelligence Outlook

deepwatch assesses that automated compromise of Internet-facing systems for the installation of crypto mining bots will continue as cryptocurrencies maintain or increase in value. Additionally, the crypto mining bots increase resource consumption on systems and may negatively impact the overall system performance. deepwatch recommends organizations to be constantly aware of their Internet-facing systems and ensure these systems are at the most current patch levels for risk reduction efforts towards this type of activity. deepwatch employs numerous detections to observe malicious file executions as well as known delivery and initial access infection vectors. deepwatch recommends determining the applicability of the IOCs listed in Appendix A and if necessary adding them to your blocklist.

Back to Table of Contents

Malware | Malware Campaign Uses Clever 'Captcha' to Bypass Browser Warning

August 17, 2021
Source: *Bleeping Computer*

Key Points:

- To lure users into downloading a malicious file a URL with an embedded YouTube video is used, once the play button is clicked Chrome's security features warn that the file may be malicious.
- To trick users into downloading the file, threat actors are using a fake reCaptcha that allows the file to be downloaded.
- Once the file is downloaded, it compiles a .NET application that launches a DLL for the Gozi malware.

Summary:
MalwareHunterTeam shared a suspicious URL with BleepingComputer that secretly downloads the Gozi malware when a user attempts to watch an embedded YouTube video about a New Jersey women's prison.

To circumvent Google Chrome's security feature a fake reCaptcha image is displayed on the screen. When a user clicks on the play button, a fake reCaptcha image prompts the user to press the B, S, Tab, A, F, and the Enter buttons on their keyboard. Once the user presses the Tab key the 'Keep' button will be highlighted, and then pressing the 'Enter' key will click on the button. This allows Chrome to download a file named console-play.exe. Once the executable runs, it creates a folder under %AppData%\Bouncy for .NET Helper and installs numerous files. All of these files are a decoy, except the BouncyDotNet.exe executable, which is launched. Once running, BouncyDotNet.exe will compile a .NET application that launches a DLL for the Gozi, aka Ursnif, banking trojan. Gozi will steal account credentials, download further malware to the computer, and execute commands issued remotely by the threat actors.

dw Threat Intelligence Outlook

Of note is that banking trojans similar to Gozi have been used in ransomware attacks as some of the most prolific trojans employ a similar business model as that of ransomware RaaS groups. deepwatch recommends warning end-users about this potential threat. In addition, deepwatch employs numerous detections to observe malicious file executions as well as known delivery and initial access infection vectors. deepwatch recommends ensuring security protection software is up-to-date and working properly and determining the applicability of the IOCs listed in Appendix A and if necessary adding them to your blocklist.

Back to Table of Contents

Appendix A

IOCs Featured This Week

Domains	
Source	**IOC**
New HolesWarm botnet targets Windows and Linux servers	m.windowsupdatesupport.org
Malware Campaign Uses Clever 'Captcha' to Bypass Browser Warning	http://ntv-play.com/video/04169823/tls/console-play.exe

Hashes		
Source	**File Name**	**IOC**
New HolesWarm botnet targets Windows and Linux servers	None given	**MD5:** dac8ab3fce07d71a63ded7a242e8f7ca 28edd00e7c4aae21a36f03200543cb76 dc076a1bd9cb0884806bc1ce95883f24 730fb51f0ad5ce4b117d6f55aa2b7b2f af07c4e9f9b6046a183d21b55bc4eaff 4a476f21d8b5b14dfcd26445733fa934 1295507537170a526985e1a40250ed36 b40eb4629d612ad14a20ed2f8fe0ba6e aab908e2a6cceef413585d706a36ce84 a27464091de77b531a44e1bed0d8cf4 **SHA256:** c0c28a3dd6955746584dae65de440a39134f3a85c 3a2f0a5db5e282302c51d8f
Malware Campaign Uses Clever 'Captcha' to Bypass Browser Warning	console-play.exe	**MD5:** a43be7341e3d13810d20b9e64e329c83 **SHA-1:** ad582a30ba365885be34fe503c744088d08b4baa **SHA-256:** e2c83783d6ab57ac91d99bfb9d607d0b5537e3056 61406bbf2347c3af92d3464

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 Operations 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