deepwatch

August 2022

INCIDENT INTEL REPORTS

Novel Backdoor Discovered

Deepwatch ATI detects and responds to never before discovered backdoor deployed using Confluence vulnerability for suspected Espionage

EXECUTIVE SUMMARY

Deepwatch's Adversary Tactics and Intelligence group (ATI) recently responded to an incident after a suspicious tool, **nb.exe** (NBTscan, a tool that scans for open NETBIOS nameservers to find open shares), was observed and escalated to the victim, an organization in the research and technical services sector, by Deepwatch Squad analysts.

Note: *To track threat activity clusters observed during incident response engagements, The Deepwatch Threat Intel Team uses Threat Activity Cluster designations (TAC-###) to track similar activity across multiple engagements. The Deepwatch Threat Intel Team tracks the activity covered in this report as TAC-040.*

ATI's thorough analysis determined that the attack occurred during the end of May over a seven day period. TAC-040 highly likely exploited a vulnerability in an Atlassian Confluence server. The evidence indicates that the threat actor executed malicious commands with a parent process of tomcat9.exe in Atlassian's Confluence directory.

After the initial compromise, the threat actor ran various commands to enumerate the local system, network, and Active Directory environment. Additionally, the threat actors used RAR and 7zip to archive files and folders from multiple directories, including registry hives. Network logs suggest TAC-040 exfiltrated around 700MBs of archived data before the victim took the server offline.

Furthermore, they dropped a never-before-seen backdoor, dubbed "Ljl Backdoor", onto the compromised server. You can read Deepwatch's complete analysis with associated observables of this file in **Part 2** of this threat report.

During ATI's investigation of this incident, an XMRig crypto-miner was observed in the forensic artifacts. Deepwatch assesses that the XMRig related artifacts could be the result of multiple threat actors based on known threat actor activity related to cryptominers. Deepwatch's technical analysis of this loader with associated observables can be read in **Part 3** of this threat report.

KEY FINDINGS

CVE-2022-26134 was highly likely exploited to gain initial access.

TAC-040 cloned numerous tools from GitHub; one tool, CrackMapExec, serves as an attack framework that contains multiple tools.

TAC-040 has the capability to create or access custom, never-before-seen malware.

It is likely that TAC-040's goal was espionage-related. However, we can not completely rule out that they were financially motivated.

Organizations that conduct research in healthcare, education, international development, and environmental and agriculture, as well as provide technical services are likely targets of this threat actor.

Note About Estimative Language: *To convey the possibility or probability of our hypothesis, the Deepwatch Threat Intel Team employs probabilistic language in our assessments. Because analytical assessments are not certain, we use terms to denote that our hypothesis has a lower or greater than even chance of possibility or probability.*

For instance, terms like unlikely, improbable, highly likely, or highly improbable denote that our hypothesis has a lower than even chance of possibility or probability. Likewise, words like likely, probable, highly likely, or highly probable indicate that our hypothesis has a higher than even chance of possibility or probability.

Moreover, a "roughly even chance" denotes that our hypothesis has a roughly 50% possibility or likelihood of occurring. In addition, terms such as "might," "could," or "may" reflect situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented.

Note About Analytic Assurance: *Weighing the following factors allows us to assign our assessments and estimates with high, moderate, or low levels of assurance: the complexity of the analytical task; the robustness, number, and applicability of analytic techniques employed, and the degree to which the results coincide; overall source reliability; the degree of corroboration and agreement amongst sources if multiple sources were available; analyst collaboration, expertise, and experience on the subject matter or topic; and finally, we account for any time pressures and deadlines faced by the analyst.*

Table of Contents

Novel Backdoor Discovered

Deepwatch ATI detects and responds to never before discovered backdoor deployed using Confluence vulnerability for suspected Espionage

Who is TAC-040?

To track threat activity clusters observed during incident response engagements, The Deepwatch Threat Intel Team uses TAC-### designations to track activity across multiple incidents. This activity includes all the tactics, techniques, and procedures (TTPs) used; infrastructure; tools and malware employed; and sector and geographic targeting. Tracking threat activity clusters enable the Threat Intel Team to link observed activity across separate incidents..

TAC-040, so far, has targeted a non-profit organization that conducts research and provides technical services in the following areas: healthcare, education, international development, and environmental and agricultural services.

Analyst Note

Although the Threat Intel Team cannot be certain of TAC-040's intentions and goals, By employing the Structured Analytic Technique of Alternative Competing Hypothesis, Deepwatch Threat intelligence analysts assess that TAC-040 motivation is likely to be espionage-related. However, we cannot completely rule out that the threat actors may be financially motivated.

Additionally, this assessment is supported by the targeting of a non-profit research organization, data staging of specific directories and files, deployment of a custom never before seen backdoor, a webshell deployment utilizing another web server technology on the same system, and the lack of lateral movement to another system for several days, suggesting they were conducting thorough reconnaissance.

Due to the threat actor(s) motivation likely being espionage-related, it is likely to target organizations that conduct research in healthcare, education, international development, environmental protection, and agriculture or that offer technical services in these fields. However, the threat actor(s) could also target organizations in other industries that operate in these fields.

The Deepwatch Threat Intel Team has developed an "Indicators or Signpost of Change" matrix to monitor any activity linked to TAC-040 that is related to intended targets and their intentions. When new developments arise, we will update our customers accordingly.

TAC-040 has demonstrated the capability to create or access a never-before-seen backdoor, but they also employ numerous open-source tools cloned from GitHub. Additionally, they used a Linode server to store exfiltrated data, which is interesting as we have not seen any open-source reporting of threat actors using Linode to store exfiltrated data.

The victim denied the threat actor the ability to laterally move within the environment by taking the server offline, potentially preventing the exfiltration of additional sensitive data and restricting the threat actor(s) ability to conduct further malicious activities. However, this limited our visibility which may have provided evidence to support whether the threat actor was motivated by financial gain or political espionage.

At this time, the Deepwatch Threat Intel Team cannot link this activity cluster with any level of assurance to any other activity clusters tracked by third parties.

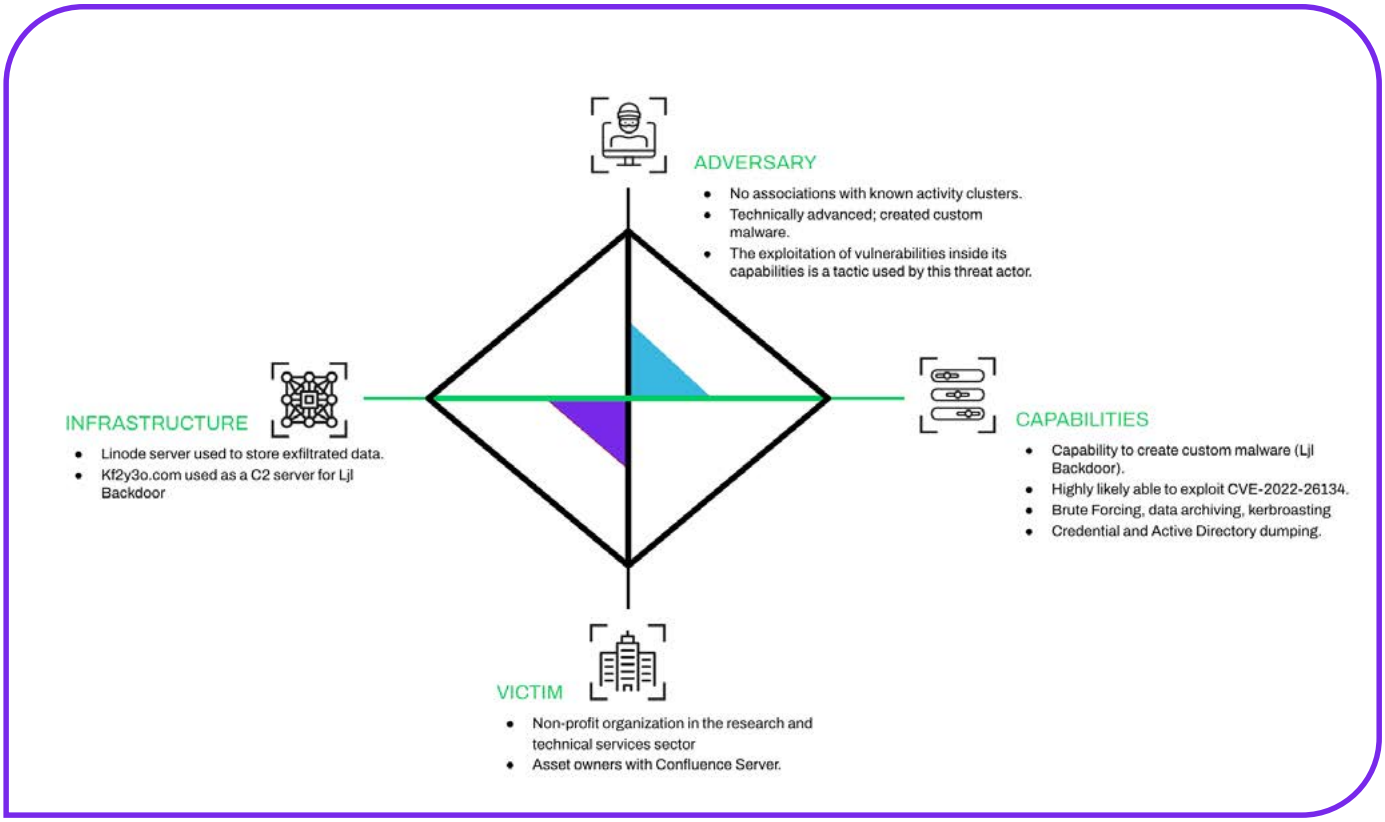


Figure1: *The first observed command executed by TAC-040*

Attack Analysis

EXPLOITATION OF CONFLUENCE

Deepwatch suspects that towards the end of May 2022, TAC-040 obtained initial access by exploiting a vulnerability [T1588.006] in an outdated Confluence server [T1190] due to the initial command TAC-040 executed (figure 1) [T1033].

> **Analyst Note**
>
> *The vulnerability is highly likely to be **CVE-2022-26134** based on the parent process and proximity to Atlassian's disclosure of the vulnerability a week later, as well as widespread exploitation of Confluence as reported by numerous third parties. .*

According to Atlassian's **security advisory**, the vulnerability affects all versions after 1.3.0 and, if successfully exploited, could allow a threat actor to conduct remote code execution (RCE) on vulnerable devices. However, due to visibility gaps, we cannot confirm this hypothesis, and there is the possibility that **CVE-2022-22965** could have been exploited instead.

```
cmd.exe /c "cd /d "C:\Windows\system32\"&amp;whoami"
```

Figure 2: *The first observed command executed by TAC-040*

Attack Analysis (continued)

SEARCHING FOR AND COLLECTING SENSITIVE DATA.

Once TAC-040 gained access, they issued several commands to enumerate the current user context, running processes, and high-value group memberships. They collected Active Directory data via CSVDE (figure 2) [T1119] and copied the output to a file named 123.csv. TAC-040 then archived 123.csv as 1.rar (figure 3). Additionally, TAC-040 executed ping sweep commands to enumerate an internal IP CIDR block, viewed the available network share drives, and tested their connectivity to Domain Controllers and hosts with names typically associated with mail and backup servers. Furthermore, TAC-040 employed the open-source tool nbtscan (nb.exe) to scan internal IP addresses for NetBIOS name information.

```
cmd.exe /c "cd /d "C:\Windows\system32\"&amp;C:\ProgramData\Git\csvde.exe -f
C:\ProgramData\Git\123.csv"
```

Figure 3: *Active Directory enumerated and copied to 123.csv*

```
C:\ProgramData\Git\rar.exe  a c:\C:\ProgramData\Git\1.rar C:\ProgramData\Git\123.csv
```

Figure 4: *123.csv archived as 1.rar*

Once the threat actors completed discovery, TAC-040 executed commands to archive [T1560.001] the HKLM\SYSTEM, HKLM\SAM, and HKLM\SECURITY (figure 4) registry hives. At this point, the threat actor listed specific directory contents from the available network shares. Additionally, the threat actor attempted to gain access to service and privileged accounts by brute force via password spraying [T1110.003] but failed at all attempts.

```
cmd.exe /c "cd /d "C:\logs\t"&amp;reg save HKLM\SAM SamBkup.hiv"
```

Figure 5: *TAC-040 archiving HKLM\SAM*

Attack Analysis (continued)

MAINTAINING ACCESS

After investigating the vulnerability used for initial access in the Confluence web application, the Deepwatch Threat Intelligence and Threat Response teams investigated the file system artifacts such as the Master File Table (MFT) and found no evidence or artifacts suggesting the threat actors wrote a traditional webshell to disk to gain persistent access via Apache's Tomcat instance in the Confluence installation directory.

Analyst Note

The threat actor likely utilized a memory-based webshell or opted to run commands directly through the exploit, as no dropper commands or forensic records of an on-disk webshell were recovered. Several open-source reports detail similar defense/detection avoidance techniques concerning the exploitation of CVE-2022-26134, but technical details on these techniques are sparse.

To achieve persistence (as memory webshells do not persist between service or system restarts and vulnerabilities can be patched), TAC-040 created a service on the compromised server named "VBoxxSDS" **[T1543.003]** that ran the executable "DrSDKcaller.exe," an executable name related to Trend Micro Maximum Security (figure 5). However, we do not know what this service did or its purpose as we could not recover this file. TAC-040 also created another service named "wscsvcs" that ran "wab.exe" (see **Part 2** of this threat report). Finally, TAC-040 dropped a custom webshell (jquery.aspx) in a subdirectory of 'C:\Web' (served by the IIS instance) and executed a script, smbclient_nthash.py.

Analyst Note

It is likely that this script (smbclient_nthash.py) is a "Pass the Hash" tool commonly used by threat actor(s) to attempt to move laterally once an account's hash is obtained. No arguments were passed to this tool. Therefore, we suspect the threat actor(s) were printing out usage instructions for potential usage later.

```
sc  create "VBoxxSDS" binpath= "C:\logs\DrSDKCaller.exe"  type= share start= auto displayname= "VirtualBox system service" depend= Tcpip
```

Figure 6: *VBoxxSDS service creation command*

NOVEL BACKDOOR

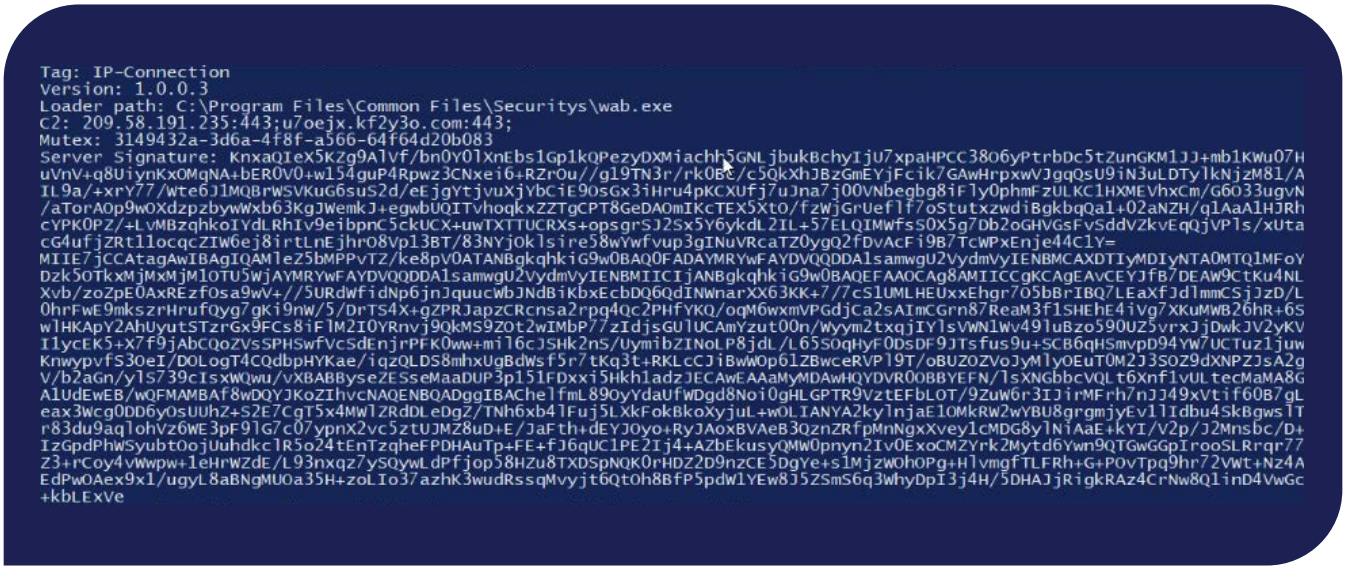
A backdoor (wab32res.dll), dubbed "ljl Backdoor", was also loaded onto the infected server. The Deepwatch Threat Intel Team has determined this backdoor is a never-before-seen and persistent backdoor **[T1587.001]**.

ljl Backdoor has the following capabilities:

- ✓ Reverse Proxy.
- ✓ Query whether the victim is active or idle.
- ✓ Exfiltrate files/directories.
- ✓ Load arbitrary and remotely downloaded .NET assemblies as "plugins."
- ✓ Get user accounts.
- ✓ Get the foreground window and window text.
- ✓ Get victim system information, such as CPU name, GPU name, hardware id, bios manufacturer,
- ✓ Mainboard name, total physical memory, LAN IP address, and mac address.
- ✓ Get victim geographic information, such as ASN, ISP, country name, country code, region name, region code, city, postal code, continent name, continent code, latitude, longitude, metro code, time zone, and date and time.

Analyst Note

*We suspect it is new, as we could not find any internal or open-source reporting on this backdoor. You can read Deepwatch's complete analysis with associated observables of this file in **Part 2** of this threat report.*



Attack Analysis (continued)

ADDITIONAL TOOLS

Once TAC-040 achieved persistence. Deepwatch observed that TAC-040 employed various publicly available open-source tools cloned from GitHub [T1588.002] (listed below). In addition, Deepwatch observed one toolset, CrackMapExec (figure 6), which serves as an attack framework with multiple tools. A security solution the victim had deployed flagged this framework as malicious.

One of these **CrackMapExec** (Figure 7) tools was used to conduct Kerberoasting [T1558.003] and AS-REP Roasting [T1558.004]. However, we could not recover the contents of the output file (output.txt), so we can not confirm if this attempt was successful. However, we do not have evidence suggesting the threat actor was able to move laterally within the network before the compromised server was brought offline.

```
git.exe  clone --recursive https://github.com/byt3bl33d3r/CrackMapExec
```

Figure 8: *Cloning CrackMapExec from GitHub*

Additionally, TAC-040 attempted password spraying [T1110.003] on numerous accounts but failed. Furthermore, the threat actor(s) attempted to join a computer to the domain using 1.py.

Analyst Note

Initial tool ingress was likely achieved by an, as yet, undetermined method to maintain access independent of the Confluence vulnerability. Deepwatch did not observe dropper or download commands that would have allowed the threat actor to download tools that would allow them to remove their dependency on Confluence for access. Yet, the later portion of the attack TAC-040 carried out did not have a parent process of tomcat9. exe, indicating there was direct access without the need to re-exploit Confluence or utilize a webshell in the installation directory.

TAC-040 demonstrated the ability to upload custom tools (all.exe and dump.dll) through an unknown method than running a traditional download cradle with the Confluence RCE vulnerability.

Attack Analysis (continued)

ADDITIONAL TOOLS

- Open-source tools cloned from GitHub:
- NetRipper
- PowerSploit
- Invoke-Vnc
- CME-PowerShell-Scripts
- CrackMapExec: attack framework with multiple tools
- Invoke-Obfuscation
- SessionGopher
- mimipenguin
- mimikittenz
- RID_Hijacking
- RandomPS-Scripts

During our investigation into this incident, a loader for an XMRig crypto-miner was observed in the forensic artifacts. Deepwatch's technical analysis of this loader with associated observables can be read in **part 3** of this threat report.

Analyst Note

Deepwatch assesses that the XMRig related artifacts could be the result of multiple threat actors based on known threat actor activity related to cryptominers.

EXFILTRATING SENSITIVE DATA

Network logs suggest around 700MBs of data was exfiltrated [T1567] to a Linode server (192.46.223[.]211) **[T1583.003]**.

Analyst Note

Based on the directories, folders, and files archived, exfiltrated data likely included an archive of the Active Directory, web configuration files, network hosts, C drive log files, and other sensitive data. However, we cannot positively confirm which archived files TAC-040 exfiltrated due to visibility gaps.

What You Need to Do

For organizations unable to upgrade Confluence immediately, Atlassian has provided a temporary workaround for the following specific product versions.

- Confluence 7.15.0 – 7.18.0
- Confluence 7.0.0 – Confluence 7.14.2

Additional risk reduction recommendations include:

- Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.
- When PowerShell is necessary, restrict PowerShell execution policy to only administrators that require it.
- Where possible, only permit the execution of signed scripts.
- Set account lockout policies after five to 10 failed login attempts to prevent passwords from being guessed and enforce multi-factor authentication.
- Make sure that all accounts have Kerberos pre-authentication enabled whenever possible and audit changes to settings.
- Restrict access to Confluence only when a user has been authenticated or only allows access from trusted sources.
- Segment Systems that are Internet exposed from the internal network to limit the impact of internal systems from being compromised.
- Ensure proper systems/applications inventory is regularly occurring, especially Internet-facing ones, for identification of systems/applications to include in a patch management program.
- Implement a patch management program with critical priority patching for systems/applications that are Internet-facing.

Observing this activity cluster may be possible by auditing and monitoring logs for the following:

- Bash, cmd.exe, or powershell.exe spawned by Apache Tomcat.
- .jsp, .jar. .asp, .aspx, or .php files being created or modified in Confluence/Bitbucket/Jira web directories.
  - It may also be possible to detect webshell installation artifacts in confluence_install_dir\work\Standalone\localhost\ROOT\org\apache\jsp\ with the naming convention NAME_jsp.java for .jsp webshells that have already been deleted.
- Unexpected service installation activity (especially those that launch .exe files in the Logs or Temp directories).
- Git clone activity and associated DNS queries/proxy logs.
- Files with short names being executed (ex. 5.exe, ad.exe).
- Executables run multiple times with a high distinct count of source paths.
  - Ex. rar.exe being run in C:\Temp, C:\Logs, and C:\Web.
- Usage of the following Live Off the Land Binaries (LOLBins): reg, net, or whoami, spawned as child processes of Apache Tomcat (Event ID 4688).
- rar.exe or 7z.exe activity on Windows and related commands on Linux
  - Especially when running in succession in multiple configuration directories or paths containing other sensitive data

Intelligence Gaps

Regarding this activity cluster, there are still a few unanswered questions. First and foremost, we cannot be certain of TAC-040's intentions and goals due to visibility gaps. However, it is likely that TAC-040's goal was espionage-related. However, we can not completely rule out that they were financially motivated. The Threat Intel Team needs additional evidence to build confidence in this hypothesis.

Secondly, the threat actor likely exploited CVE-2022-26134. However, there are other vulnerabilities, albeit unlikely, that the actor could have exploited. Unfortunately, visibility gaps prevent us from confirming which vulnerability TAC-040 exploited.

Thirdly, we could not recover many tools, and scripts dropped on the server by TAC-040 or determine how they were dropped. Therefore, we are unable to assess their purpose and capabilities.

Conclusion

TAC-040 highly likely exploited CVE-2022-26134 in an outdated Confluence server, highlighting the importance for organizations to apply patches as soon as possible and ensure that systems and servers that contain sensitive information are not exposed to the internet. One item to note is that TAC-040 created or had access to a never-before-seen backdoor, which we analyzed in **Part 2** of this report.

Additionally, TAC-040 archived the Active Directory and several sensitive files and cloned numerous tools from GitHub. Targeting a non-profit research organization, archiving of Active Directory, registry hives, and the suspected contents of other sensitive files suggest that TAC-040 may have an espionage mandate. However, we can not completely rule out that they may be financially motivated.

Therefore, organizations that conduct research in healthcare, education, international development, and environmental and agriculture or provide technical services in these areas are likely targets of this threat actor. However, organizations in other sectors that operate in these areas may also be targets.

Deepwatch immediately alerts customers when new threats occur or who have been targeted or attacked, giving them the tools and actionable intelligence they need to safeguard their environments. We encourage organizations to share our threat intelligence reports with other teams or colleagues, including our weekly Cyber Intel Briefs and Customer Advisories.

Deepwatch Threat Intel Team has moderate assurance in our overall analysis of this threat. The data is sourced from our internal collections. However, no additional corroborating sources were available for the assessment, and analysts' estimations are based on available data. Furthermore, the analytic task was moderately complex, and analysts' collaborated and employed a few structured analytical techniques and were afforded sufficient time to complete the analysis.

deepwatch

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's fastest, most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

Visit www.deepwatch.com to learn more.

CONTACT US

4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
(855) 303-3033

MITRE ATT&CK

T1583.003	Acquire Infrastructure: Virtual Private Server
T1588.006	Obtain Capabilities: Vulnerabilities
T1588.002	Obtain Capabilities: Tool
T1587.001	Develop Capabilities: Malware
T1190	Exploit Public-Facing Application
T1033	System Owner/User Discovery
T1119	Automated Collection
T1560.001	Archive Collected Data: Archive via Utility
T1110.003	Brute Force: Password Spraying
T1543.003	Create or Modify System Process: Windows Service
T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting
T1558.004	Steal or Forge Kerberos Tickets: AS-REP Roasting
T1567	Exfiltration Over Web Service

Observables

Note: Observables are properties (such as an IP address, MD5 hash, or the value of a registry key) or measurable events (such as creating a registry key or a user) and are not indicators of compromise. The observables listed below are intended to provide contextual information only. Deepwatch evaluates the observables and applies those it deems appropriate to our detections.

Observing sets of these properties (observables) could indicate compromise. For instance, observing an IP address, the creation of a user with admin privileges, and a registry key could be indicators of compromise and should be investigated further.

Webshell (jquery.aspx)
SHA256: 3fe094bab0e6c93a9a99a2dce75c60c5f3526ac786bb8b551534f098fa1419d3

1.py
SHA256: cbea88a0fcef3a157ca83582f152e3a67257c6de22ecdda025db78d94dead1c1

nb.exe
SHA256: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

wab.exe (ljl Backdoor)
SHA256: 112d5f4755154d7b1ac6f5c0c84a2b0dfb053bd6c308e23dfd96b9206f105e40

wab32res.dll (ljl Backdoor)
SHA256: f2dfe17f992072266ac57835432b56834657ea0e75eb42fb9a034b3e517f3e25

Linode Server
192.46.223[.]211

IP that communicated with nb.exe
205.185.121[.]53 (Frantech)

Files and Commands Executed by TAC-040:

- c:\users\public\all.exe
- c:\users\public\dump.dll
- c:\Windows\System32\query.exe user
- c:\Windows\System32\cmd.exe /c “cd /d “C:\Windows\system32\”&c:\users\public\rar.exe a
- c:\users\public\d.rar c:\users\public\1.bin”
- c:\Windows\System32\PING.EXE www.google.com
- c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe echo ((new-object Net.Sockets.TcpClient).Connect(\”INTERNAL_IP\”,636)) “open!”
- c:\Windows\System32\cmd.exe /c “cd /d “C:\Windows\system32\”&ping -n 1 HOSTNAME”
- c:\Windows\System32\cmd.exe /c “cd /d “C:\logs\t”&”C:\Program Files\7-Zip\7z.exe” -t7z a 1.7z .*.hiv -mx9”
- c:\Windows\System32\net.exe user USER /domain
- c:\ProgramData\Git\DATE\mbae-svc.exe kerberoast /domain:DOMAIN /dc:HOSTNAME /outfile:1.txt
- c:\Windows\System32\cmd.exe /c “cd /d “C:\Windows\system32\”&net view \\HOSTNAME”
- c:\Windows\System32\cmd.exe /c “cd /d “C:\Windows\system32\”&net group “Enterprise Key Admins” /domain”
- c:\logs\DrSDKCaller.exe
- c:\Windows\System32\sc.exe create “VBoxxSDS” binpath= “C:\logs\DrSDKCaller.exe” type= share start= auto displayname= “VirtualBox system service” depend= Tcpip
- c:\logs\Python39\python.exe 1.pyá-dc “HOSTNAME” -dc-ip “INTERNAL_IP” -computer-name “HOSTNAME” FILE_NAME.ns/USER:”PASSWORD”
- C:\Windows\System32\cmd.exe /c “cd /d “C:\logs”&for /l %b in (1,1,255) do ping x.x.x.%b -n 1 >>t.txt”
- C:\Windows\System32\cmd.exe /c “cd /d “C:\Windows\system32\”&net localgroup administrators”
- C:\PerfLogs\magick.exe -l tcp -p 445,443 INTERNAL_SUBNET
- “C:\logs\Python39\python.exe” “C:\logs\Python39\Scripts\pipx.exe” install crackmapexec