IT threat evolution in Q2 2023

securelist.com/it-threat-evolution-q2-2023/110355/

Authors

 David Emm

Targeted attacks

Gopuram backdoor deployed through 3CX supply-chain attack

Earlier this year, a Trojanized version of the 3CXDesktopApp, a popular VoIP program, was used in a high-supply-chain attack. The attackers were able to embed malicious code into the *libffmpeg* media processing library to download a payload from their servers.

When we reviewed our telemetry on the campaign, we found a DLL on one of the computers, named guard64.dll, which was loaded into the infected 3CXDesktopApp.exe process. A DLL with this name was used in recent deployments of a backdoor that we dubbed Gopuram, which we had been tracking since 2020. While investigating an infection of a cryptocurrency company in Southeast Asia, we found Gopuram coexisting on target computers with AppleJeus, a backdoor attributed to the Lazarus.

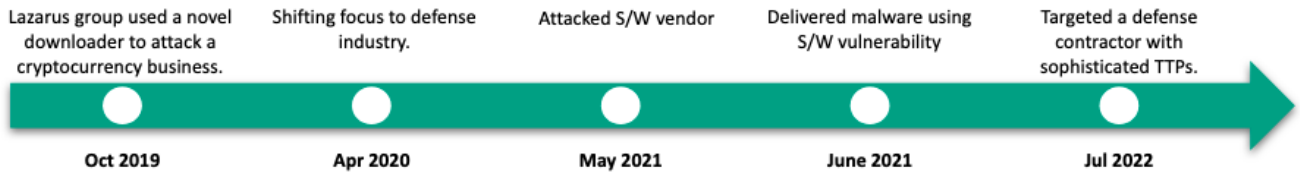
We had observed few victims compromised using Gopuram, but the number of infections increased in March 2023 — a spike that was directly related to the 3CX supply chain attack. The threat actor specifically targeted cryptocurrency companies. The backdoor implements commands that allow the attackers to interact with the victim's file system and create processes on the infected machine. Gopuram was additionally observed to launch in-memory modules.

The fact that Gopuram backdoor has been deployed to less than 10 infected computers indicates that the attackers used Gopuram with surgical precision. We observed that they have a specific interest in cryptocurrency companies. We also learned that the threat actor behind Gopuram infects target machines with the full-fledged modular Gopuram backdoor. We believe that Gopuram is the main implant and the final payload in the attack chain.

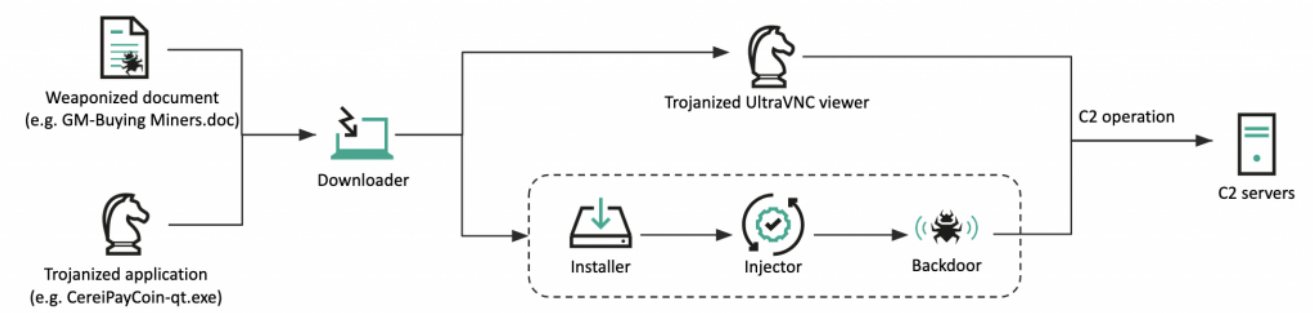
The discovery of the new Gopuram infections allowed us to attribute the 3CX campaign to the Lazarus threat actor with medium to high confidence.

Tracking the Lazarus DeathNote campaign

Lazarus is a notorious and highly skilled threat actor. Over the last few years we have tracked DeathNote, one of Lazarus's active clusters, observing a shift in the threat actor's targets as well as the development and refinement of its TTPs (Tactics, Techniques, and Procedures).



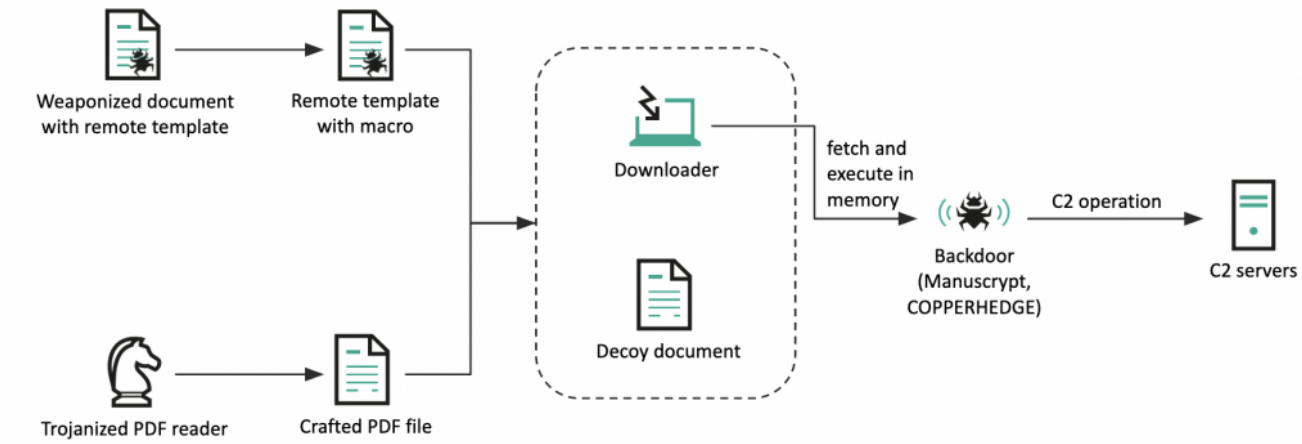
Since 2018, Lazarus has persistently targeted crypto-currency-related businesses for a long time, using malicious Word documents and themes related to the crypto-currency business to lure potential targets. If the target opened the document and enabled the macros, a malicious script would extract the embedded downloader and load it with specific parameters. Lazarus used two different kinds of second-stage payload in these attacks: the first, a Trojanized application masquerading as the UltraVNC viewer, the second, a typical multi-stage backdoor.



Our investigations identified compromised individuals or companies in Cyprus, the US, Taiwan, and Hong Kong.

In April 2020, we uncovered a significant shift in targeting and infection vector. The DeathNote cluster was used to target the automotive and academic sectors in Eastern Europe, both of which are connected to the defense industry. At this point, the threat actor switched all the decoy documents to job descriptions related to defense contractors and diplomatic services.

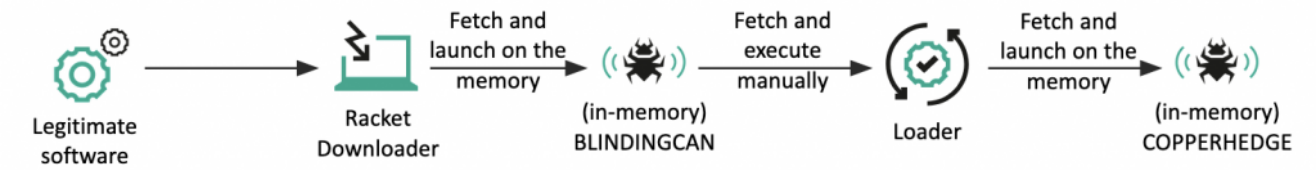
Lazarus also refined its infection chain using the remote template injection technique in its weaponized documents, as well as utilizing Trojanized open-source PDF viewer software. Both infection methods resulted in the same malware (the DeathNote downloader), which uploaded the target's information and retrieved the next-stage payload at the discretion of the C2 (Command and Control) server. Finally, a COPPERHEDGE variant was executed in memory.



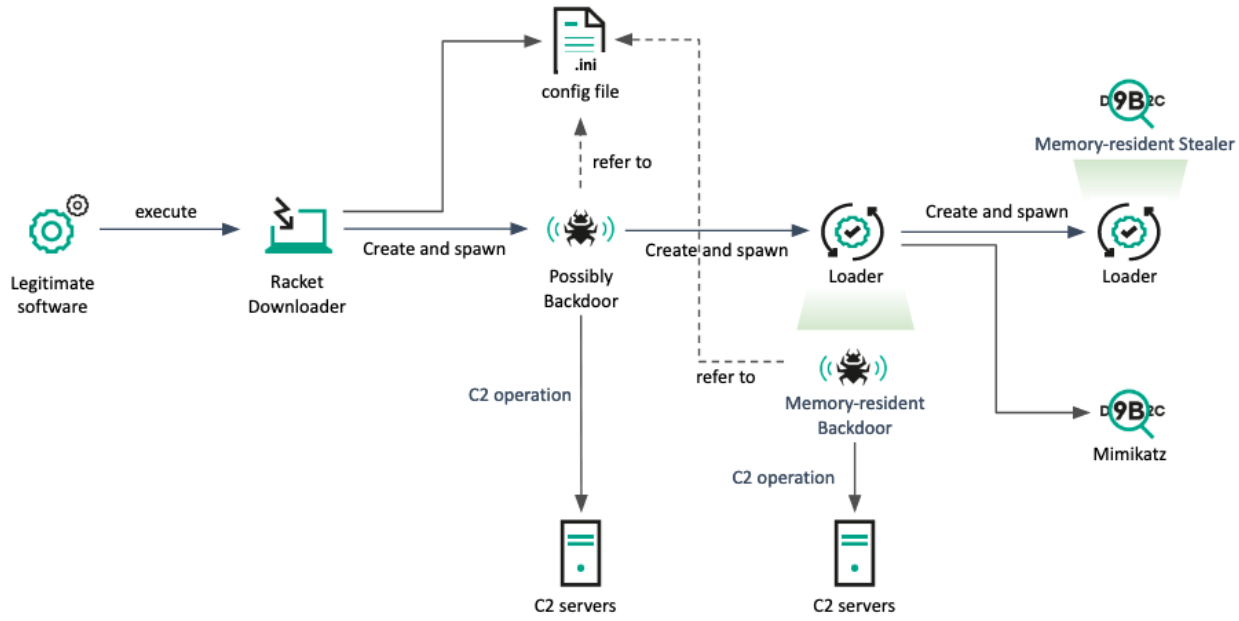
In May 2021, the DeathNote cluster was used to compromise a European IT company providing solutions for monitoring network devices and servers, possibly because Lazarus had an interest in this company's widely-used software or its supply-chain.

In early June 2021, the Lazarus group began utilizing a new infection mechanism against targets in South Korea. One thing that caught our attention was that the initial stage of the malware was executed by a legitimate security software that is widely used in the country. It's thought that the malware was spread through a vulnerability in the software.

As in the previous case, the initial infection vector created the downloader malware. Once connected to the C2 server, the downloader retrieved an additional payload based on the operator's commands and executed it in memory. During this time, the BLINDINGCAN malware was used as a memory-resident backdoor. While the BLINDINGCAN malware has sufficient capabilities to control the victim, the actor manually implanted additional malware: it's thought that the group aimed to create an auxiliary method to control the victim. Finally, the COPPERHEDGE malware, previously used by this cluster, was executed on the victim.



A year later, in March 2022, we discovered that the same security program had been exploited to propagate similar downloader malware to several victims in South Korea. However, a different payload was delivered in this case. The C2 operator manually implanted a backdoor twice, and although we were unable to acquire the initially implanted backdoor, we assume it is the same as the backdoor in the following stage. The newly implanted backdoor is capable of executing a retrieved payload with named-pipe communication. In addition, the actor utilized side-loading to execute Mimikatz and used stealer malware to collect keystroke and clipboard data from users.



At around the same time, we uncovered evidence that one defense contractor in Latin America had been compromised by the same backdoor. The initial infection vector was similar to what we've seen with other defense industry targets, involving the use of a Trojanized PDF reader with a crafted PDF file. However, in this particular case, the actor adopted a side-loading technique to execute the final payload. When the malicious PDF file is opened with the Trojanized PDF reader, the victim is presented with the same malware mentioned above, which collects and reports the victim's information, retrieves commands and executes them using pipe communication mechanisms. The threat actor used this malware to implant additional payloads, including legitimate files for side-loading purposes.

In July 2022, Lazarus successfully breached a defense contractor in Africa. The initial infection was a suspicious PDF application, which had been sent via the Skype messenger. After executing the PDF reader, it created both a legitimate file (CameraSettingsUIHost.exe) and a malicious file (DUI70.dll) in the same directory. This attack relied heavily on the same DLL side-loading technique that we observed in the previous case. Lazarus used this malware several times in various campaigns; and also used the same DLL side-loading technique to implant additional malware that is capable of backdoor operation. In order to move laterally across systems, the actor used an interesting technique called ServiceMove. This technique uses the Windows Perception Simulation Service to load arbitrary DLL files: by creating an arbitrary DLL in C:\Windows\System32\PerceptionSimulation\ and starting the service remotely, the threat actor was able to achieve code execution as NT AUTHORITY\SYSTEM on a remote system.

Our analysis of the DeathNote cluster reveals a rapid evolution in its TTPs over the years. As Lazarus continues to refine its approaches, it is crucial for organizations to maintain vigilance and take proactive measures to defend against its malicious activities. By staying informed

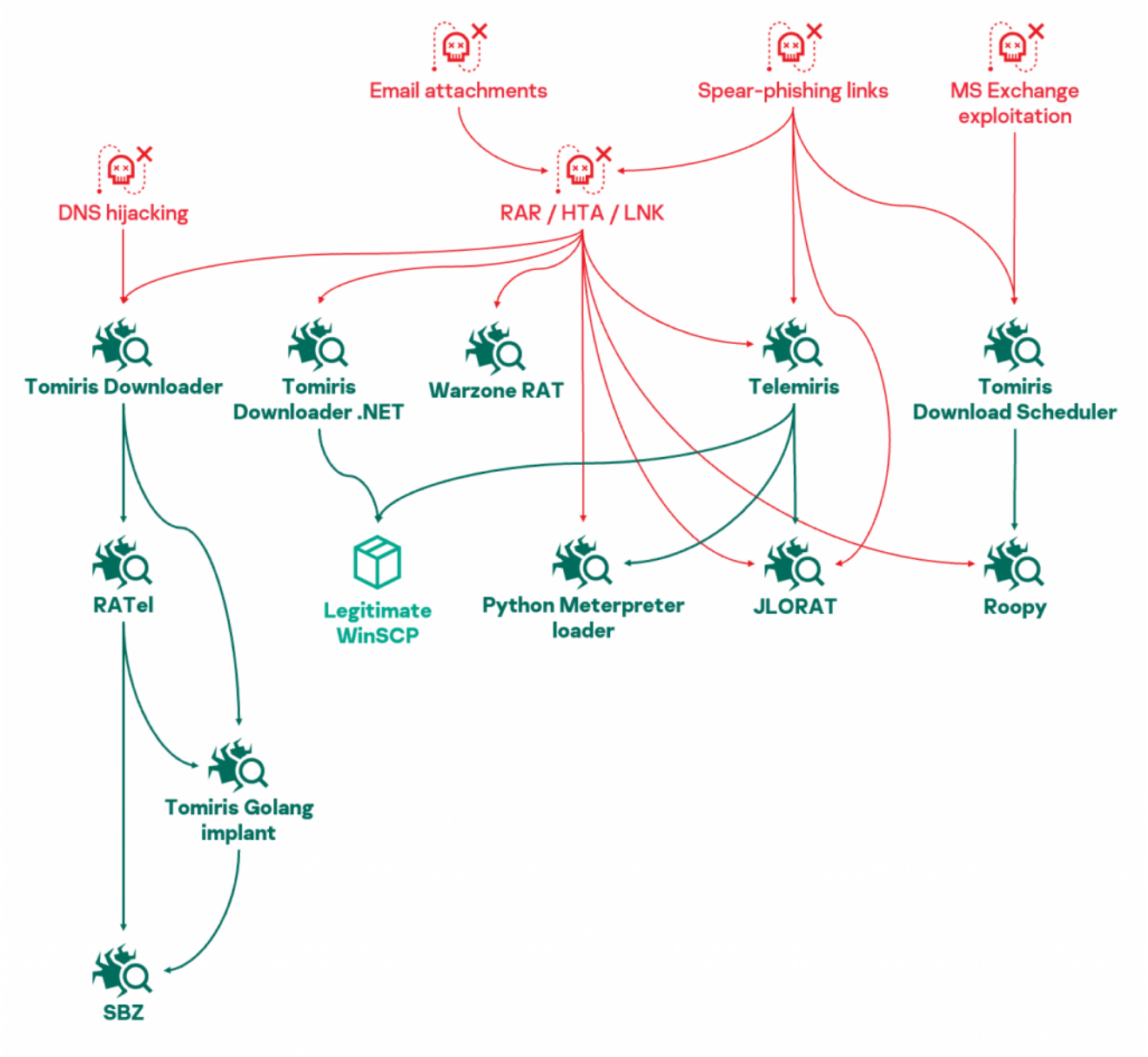
and implementing strong security measures, organizations can reduce the risk of falling victim to this dangerous adversary.

Tomiris called, they want their Turla malware back

We first reported Tomiris in September 2021, following our investigation into a DNS hijack against a government organization in the CIS (Commonwealth of Independent States). We described links between a Tomiris Golang implant and SUNSHUTTLE (which has been linked to NOBELIUM/APT29/TheDukes) as well as Kazuar (which has been linked to Turla). However, interpreting these connections proved difficult. We have continued to track Tomiris as a separate threat actor over three new attack campaigns between 2021 and 2023, and our telemetry has allowed us to shed more light on this group.

This threat actor's activities have been focused on CIS members and Afghanistan: while we identified a few targets in other locations, all of them appear to be foreign diplomatic entities of these countries.

Tomiris uses a wide variety of malware implants developed at a rapid pace and in all programming languages imaginable. The tools used by this threat actor fall into three categories: downloaders, backdoors, and file stealers. The threat actor not only develops its own tools, but also uses open source or commercially available implants and offensive tools. Tomiris employs a wide variety of attack vectors: spear-phishing, DNS hijacking, exploitation of vulnerabilities (specifically ProxyLogon), suspected drive-by downloads, and other "creative" methods.



The attribution of tools used in a cyber-attack can sometimes be a very tricky issue. In January, some fellow researchers attributed an attack on organizations in Ukraine to Turla, based, at least in part, on the use of KopiLuwak and QUIETCANARY (which we call TunnusSched) — malware known to have been used by Turla.

We discovered that a TunnusSched sample had been delivered to a government target in the CIS in September 2022; and our telemetry indicated that this malware had been deployed from Tomiris's Telemiris malware. Moreover, starting in 2019, we discovered additional implant families linked to KopiLuwak; and that TunnusSched and KopiLuwak are part of the same toolset.

We remain convinced that, despite possible ties between the two groups, Turla and Tomiris are separate threat actors. Tomiris is undoubtedly Russian-speaking, but its targeting and tradecraft are significantly at odds with what we have observed for Turla. In addition, Tomiris's general approach to intrusion and limited interest in stealth are significantly at odds with documented Turla tradecraft.

This throws up several possibilities.

1. Turla is happy to use a tool that was burned in 2016; and is still using it in current operations along with new tools.
2. Other threat actors may have repurposed these tools and are using them under a false flag.
3. Turla shares tools and expertise with Tomiris, or cooperates with Tomiris on joint operations.
4. Tomiris and Turla rely on a common supplier that provides offensive capabilities. Or maybe Tomiris initially started out as a private outfit writing tools for Turla and is now branching out into the mercenary business.

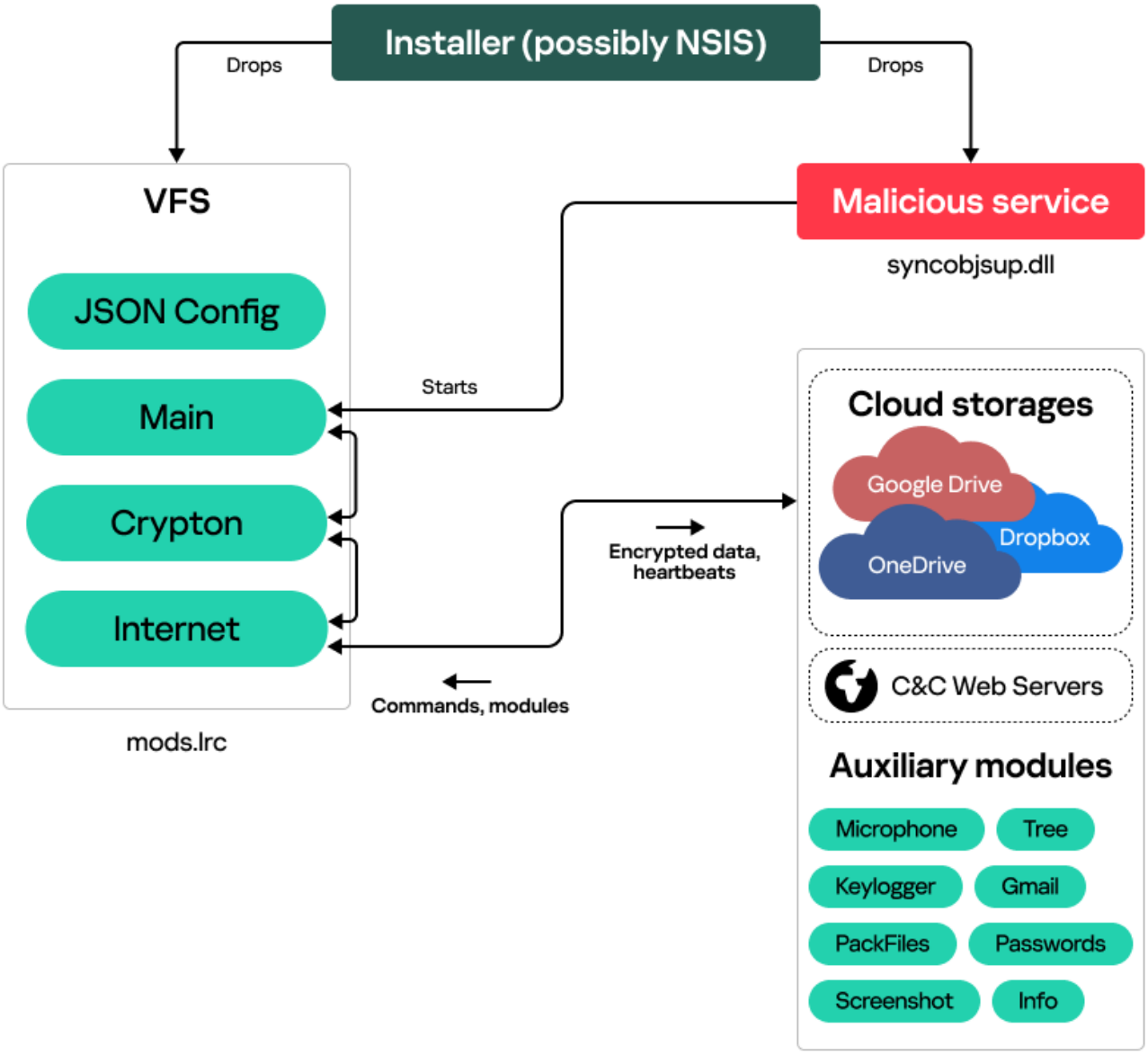
Our assessment is that the first two hypotheses are the least likely and that there exists a form of deliberate co-operation between Tomiris and Turla, although its exact nature is hard to determine with the information we have at hand.

CloudWizard APT: the bad magic story goes on

Last October, we identified an active infection of government, agriculture, and transportation organizations located in Donetsk, Lugansk, and Crimea. We published the results of our initial investigations into the PowerMagic and CommonMagic implants in March. At that time, we were unable to find anything to connect the samples we found and the data used in the campaign to any previously known threat actor. However, our continuing investigations revealed more information about this threat, including links to other APT campaigns.

While looking for implants bearing similarities to PowerMagic and CommonMagic, we identified a cluster of even more sophisticated malicious activities originating from the same threat actor. Interestingly, the targets were located not only in the Donetsk, Lugansk, and Crimea regions, but also in central and western Ukraine. These targets included individuals, as well as diplomatic and research organizations.

The newly discovered campaign involved use of a modular framework we dubbed CloudWizard. Its features include taking screenshots, microphone recording, keylogging, and more.



There have been many APT threat actors operating in the Russo-Ukrainian conflict region over the years, including Gamaredon, CloudAtlas, and BlackEnergy. So we looked for clues that might allow us to attribute CloudWizard to a known threat actor. CloudWizard reminded us of two campaigns observed in Ukraine and reported publicly: Operation Groundbait (first described by ESET in 2016) and Operation BugDrop (discovered by CyberX in 2017). While there have been no updates about Prikormka malware (part of Operation Groundbait) for a few years now, we discovered multiple similarities between the malware used in that campaign and CommonMagic and CloudWizard. It's clear, therefore, that the threat actor behind these two operations has not ceased its activity and has continued developing its cyber-espionage toolset and infecting targets of interest for more than 15 years.

Meet the GoldenJackal APT group. Don’t expect any howls

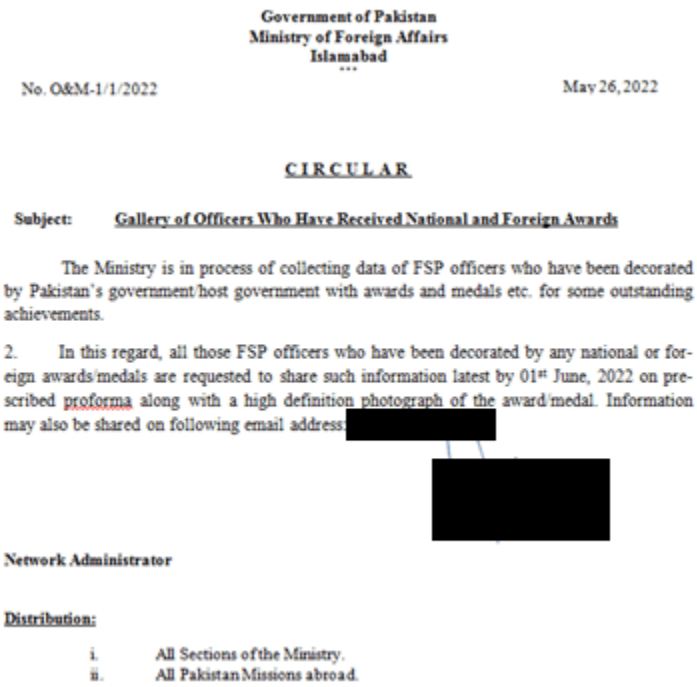
GoldenJackal, an APT group that has been active since 2019, typically targets government and diplomatic entities in the Middle East and South Asia.

We started monitoring this threat actor in mid-2020 and have observed a constant level of activity that indicates a capable and stealthy actor.

The main feature of this group is a specific toolset of .NET malware: JackalControl, JackalWorm, JackalSteal, JackalPerInfo, and JackalScreenWatcher. These implants are intended to control target computers, spread using removable drives, exfiltrate data, steal credentials, collect information about the local system and the target’s web activities, and take screen captures.

While we have limited visibility into this threat actor’s infection vectors, during our investigations, we observed the use of fake Skype installers and malicious Word documents.

The fake Skype installer was a .NET executable file named skype32.exe — a dropper containing two resources: the JackalControl Trojan and a legitimate Skype for Business standalone installer. The malicious document, which masquerades as a legitimate circular distributed to collect information about officers decorated by the Pakistan government, uses the remote template injection technique to download a malicious HTML page, which exploits the Follina vulnerability.



Government of Pakistan
Ministry of Foreign Affairs
Islamabad

No. O&M-1/1/2022 May 26, 2022

CIRCULAR

Subject: Gallery of Officers Who Have Received National and Foreign Awards

The Ministry is in process of collecting data of FSP officers who have been decorated by Pakistan's government/host government with awards and medals etc. for some outstanding achievements.

2. In this regard, all those FSP officers who have been decorated by any national or foreign awards/medals are requested to share such information latest by 01st June, 2022 on prescribed proforma along with a high definition photograph of the award/medal. Information may also be shared on following email address: [redacted]

Network Administrator

Distribution:

i. All Sections of the Ministry.
ii. All Pakistan Missions abroad.

GoldenJackal activity is characterized by the use of compromised WordPress websites as a method to host C2-related logic. We believe the attackers upload a malicious PHP file that is used as a relay to forward web requests to another backbone C2 server. We don't have any evidence of the vulnerabilities used to compromise the sites. However, we did observe that many of the websites were using obsolete versions of WordPress and some had also been defaced or infected with previously uploaded web shells, probably as a result of low-key hacktivist or cybercriminal activity.

Operation Triangulation

Early in June, we issued an early warning of a long-standing campaign that we track under the name Operation Triangulation, involving a previously unknown iOS malware platform distributed via zero-click iMessage exploits.

The attack is carried out using an invisible iMessage with a malicious attachment. Using a number of vulnerabilities in iOS, the attachment is executed and installs spyware. The deployment of the spyware is completely hidden and requires no action from the person being targeted. The spyware then quietly transmits private information to remote servers — including microphone recordings, photos from instant messengers, geo-location, and data about a number of other activities of the owner of the infected device.

We detected this threat using the Kaspersky Unified Monitoring and Analysis Platform (KUMA) — a native SIEM solution for security information and event management. Further investigation revealed that several dozen iPhones of Kaspersky employees were infected.

In addition to reaching out to industry partners to assess the prevalence of this threat, we provided a forensic methodology to help readers determine whether their organization is targeted by the unknown group behind these attacks. We subsequently published a utility to check for Indicators of Compromise (IoCs).

Following this, we released the first of a series of additional reports describing the final payload in the infection chain: a highly sophisticated spyware implant that we dubbed "TriangleDB". Operating in memory, this implant periodically communicates with the C2 infrastructure to receive commands. The implant allows attackers to browse and modify device files, get passwords and credentials stored in the keychain, retrieve geo-location information, as well as execute additional modules, further extending their control over the compromised devices.

Andariel's mistakes and a new malware family

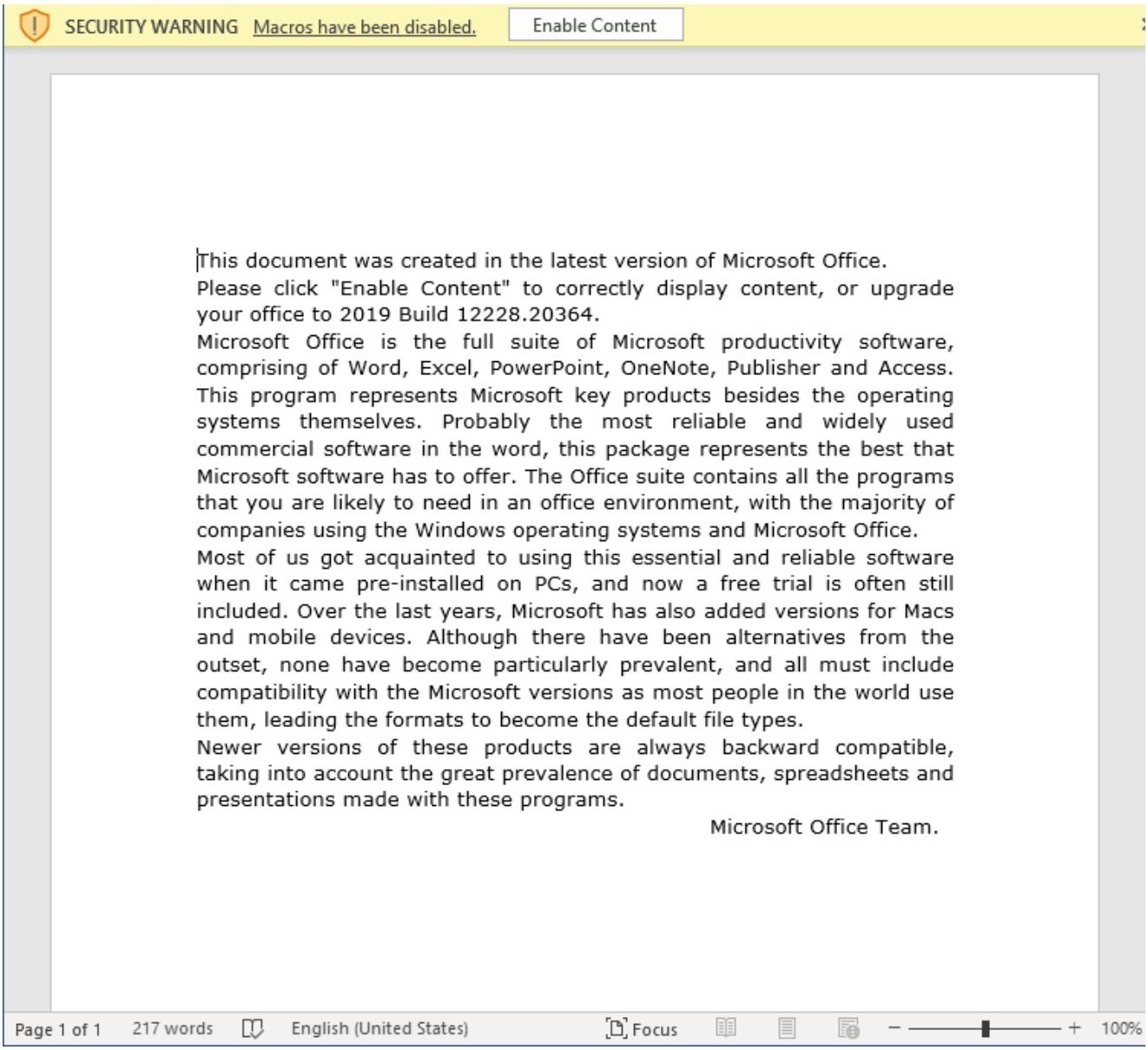
Andariel, part of the Lazarus group, is known for its use of the DTrack malware and Maui ransomware in mid-2022. During the same period, Andariel also actively exploited the Log4j vulnerability. The campaign introduced several new malware families, such as YamaBot and MagicRat, but also updated versions of NukeSped and DTrack.

While on an unrelated investigation, we stumbled upon a new campaign and decided to dig a little bit deeper. We discovered a previously undocumented malware family and an addition to Andariel's set of TTPs.

Andariel infects machines by executing a Log4j exploit, which, in turn, downloads further malware from the C2 server. Unfortunately, we were unable to catch the first piece of malware they downloaded, but we did see that exploitation was closely followed by the download of the DTrack backdoor.

We were able to reproduce the commands the attackers executed and it quickly became clear that the commands were run by a human operator — and, judging by the number of mistakes and typos, probably an inexperienced one. We were also able to identify the set of off-the-shelf tools Andariel installed and ran during the command execution phase, and then used for further exploitation of the target. These include Supremo remote desktop, 3Proxy, Powerline, Putty, Dumpert, NTDSDumpEx, and ForkDump.

We also uncovered new malware, called EarlyRat. We had first noticed this in one of the aforementioned Log4j cases and assumed it was downloaded via Log4j. However, when we started hunting for more samples, we found phishing documents that ultimately dropped EarlyRat.



EarlyRat, like the phishing document, is very simple: it is capable of executing commands, but nothing else of interest.

Other malware

Nokoyawa ransomware attacks using Windows zero-day

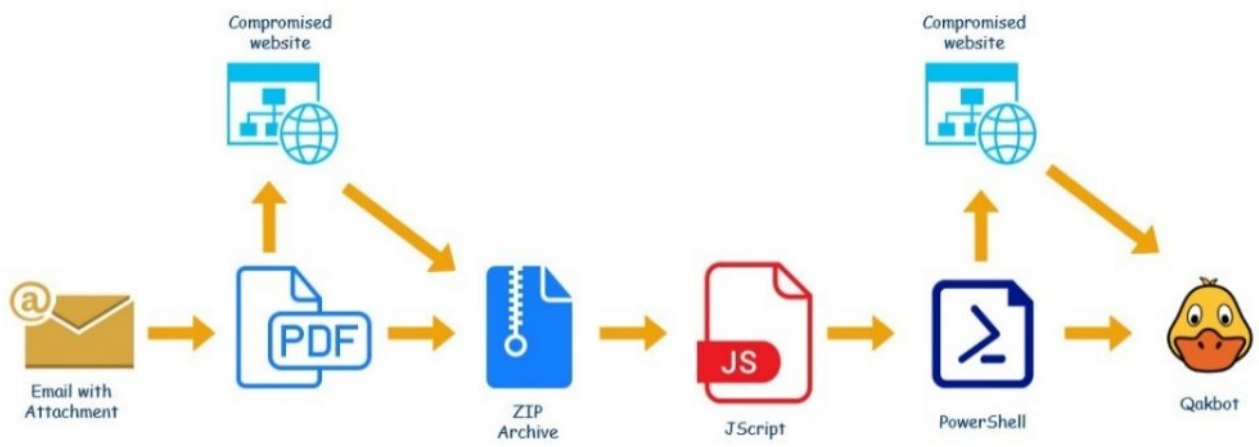
Our Behavioral Detection Engine and Exploit Prevention components detected attempts to execute elevation-of-privilege exploits on Windows servers belonging to SMBs in the Middle East, North America, and Asia. They were similar to exploits in the Common Log File System (CLFS) — the Windows logging subsystem — that we had analyzed previously. However, when we double-checked, one of them turned out to be a zero-day supporting different

versions and builds of Windows, including Windows 11. We shared our findings with Microsoft, which designated the vulnerability as CVE-2023-28252. The vulnerability was patched on April 4.

Most zero-days that we have discovered in the past were used by APT threat actors, but this one was used by Nokoyawa, a sophisticated cybercrime group, to carry out ransomware attacks.

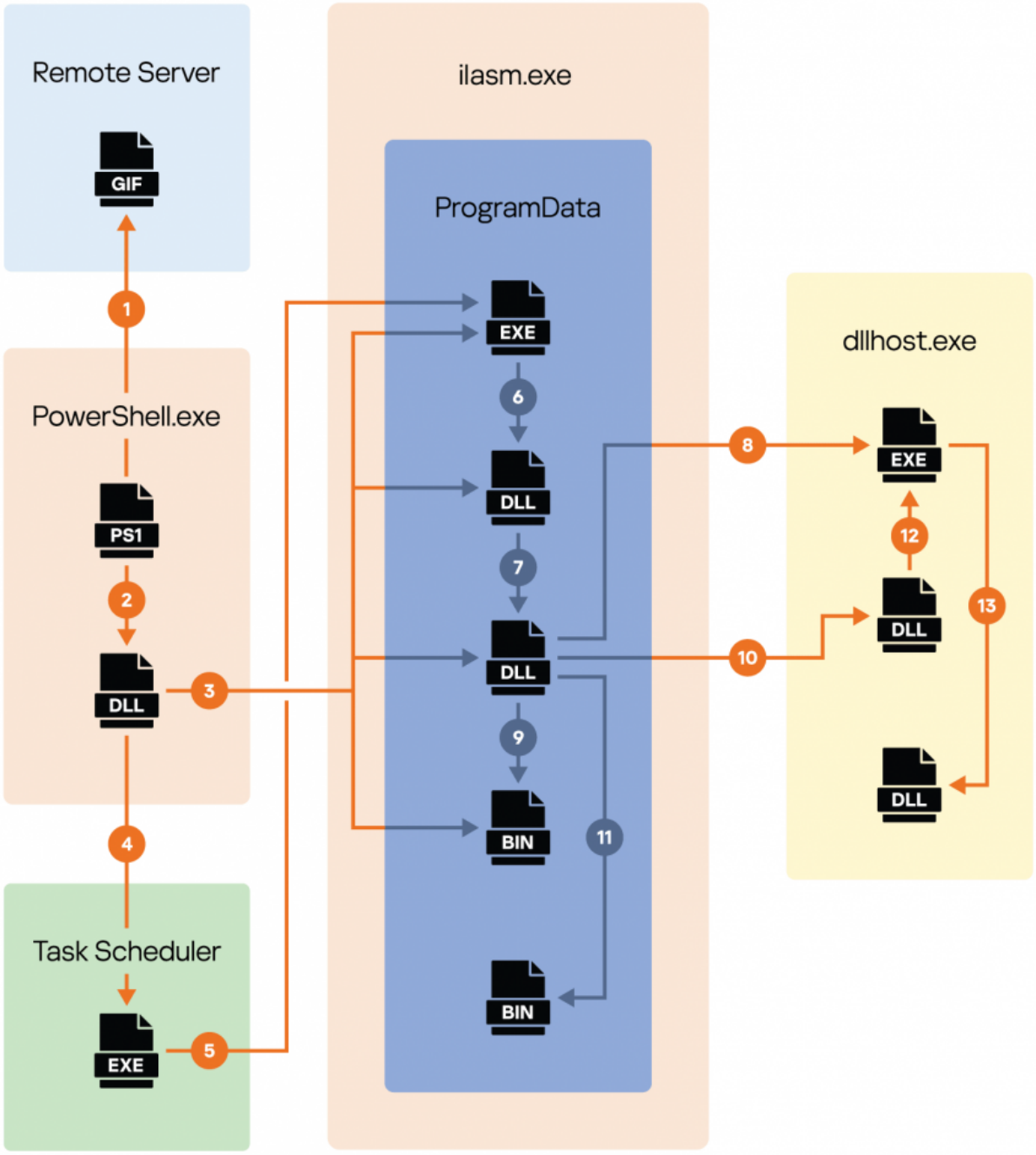
A spike in QBot banking Trojan infections

In early April, we detected a significant increase in attacks using the QBot malware (aka QakBot, QuackBot, and Pinkslipbot). The malware was delivered through malicious documents attached to business correspondence. The hackers would obtain access to real business correspondence (QBot, among other things, steals locally stored e-mails from previous targets' computers) and join the dialogue, sending messages as if they're carrying on an old conversation. The e-mails attempt to convince targets to open an attached PDF file, passing it off as an expenses list or other business matter. The PDF actually contains a fake notification from Microsoft Office 365 or Microsoft Azure. The attackers use this to try to get the target to click on the "Open" button, which then downloads a password-protected archive with the password in the text of the notification. If the recipient unpacks the archive and runs the .WSF (Windows Script File) inside, it downloads the QBot malware from a remote server.



Minas: on the way to complexity

In June 2022, we found a suspicious shellcode running in the memory of a system process. From our reconstruction of the infection chain, we determined that it originated by running an encoded PowerShell script as a task, which we believe with low confidence was created through a GPO (Group Policy Object) — something that's especially worrying, since it indicates that the attackers had compromised the target network.



The malware, which we call Minas, is a miner. It aims to hide its presence on infected systems through encryption, the random generation of names, and the use of hijacking and injection techniques. It also has the ability to stay on the infected system using persistence techniques.

We think it's very likely that a new variant will be released in the future that seeks to avoid anti-virus detection — which is why it's essential to use a security solution that doesn't primarily rely on signature detection, but also uses behavioral detection methods.

Satacom delivers browser extension that steals crypto-currency

In June, we reported a recent malware distribution campaign related to the Satacom downloader. The main purpose of the dropped malware is to steal bitcoins from the target's account by performing web injections into targeted crypto-currency websites. The malware attempts to do this by installing an extension for Chromium-based web browsers, which later communicates with its C2 server, whose address is stored in the BTC transaction data.

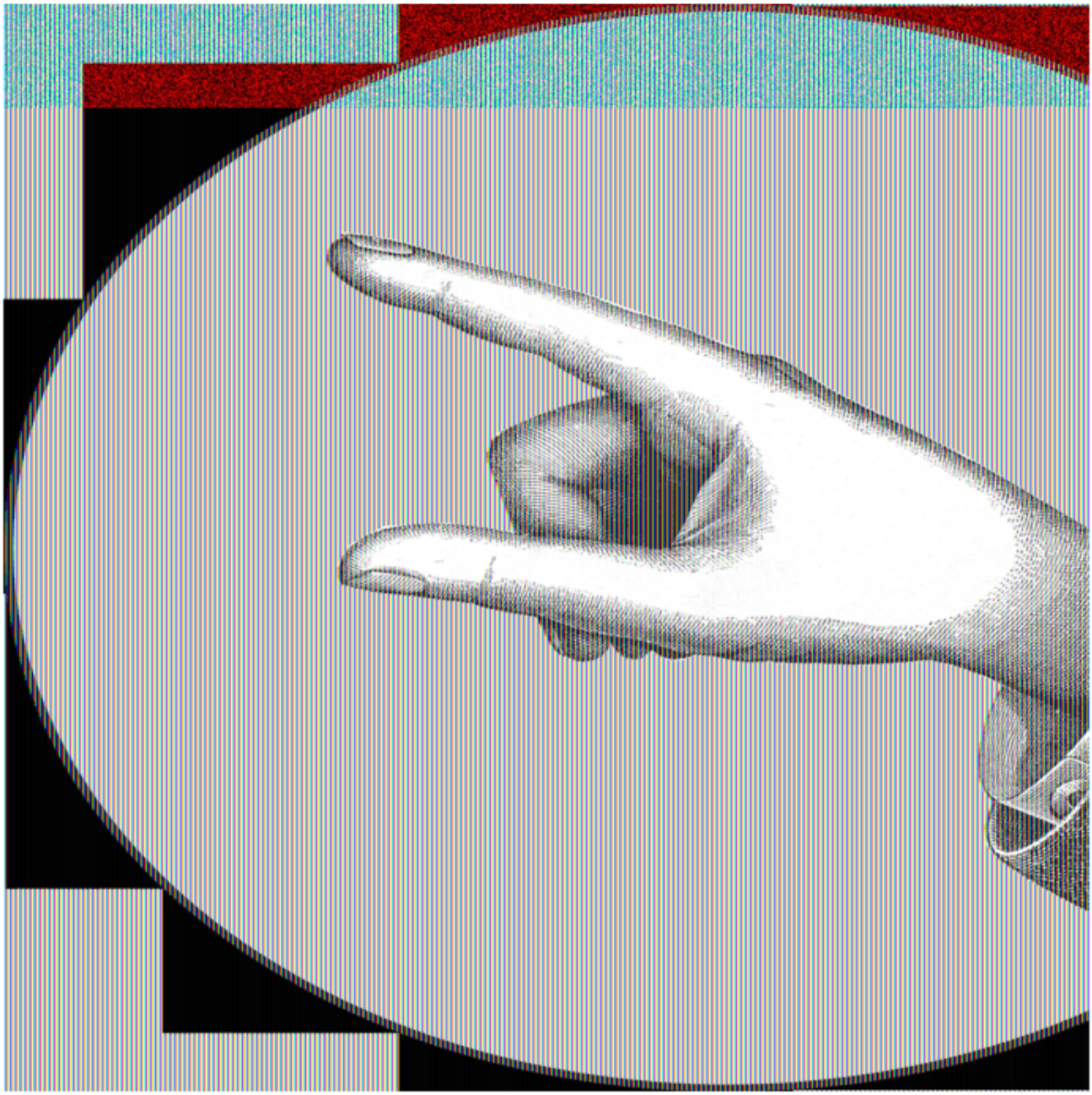
The malicious extension has various JS scripts to perform browser manipulations while the user is browsing the targeted websites, including enumeration and manipulation with crypto-currency websites. It also has the ability to manipulate the appearance of some e-mail services, such as Gmail, Hotmail, and Yahoo, in order to hide its activity.

While we analyzed a Windows-specific infection-chain, the malware operates as a browser extension, so it could be installed in Chromium-based browsers on various platforms — allowing the attackers to target Linux and macOS if they choose to do so.

DoubleFinger used to steal crypto-currency

In June, we reported the use of a sophisticated attack using the DoubleFinger loader to install a crypto-stealer and remote access Trojan. The technical nature of the attack, and its multi-stage infection mechanism, resemble attacks by APT threat actors.

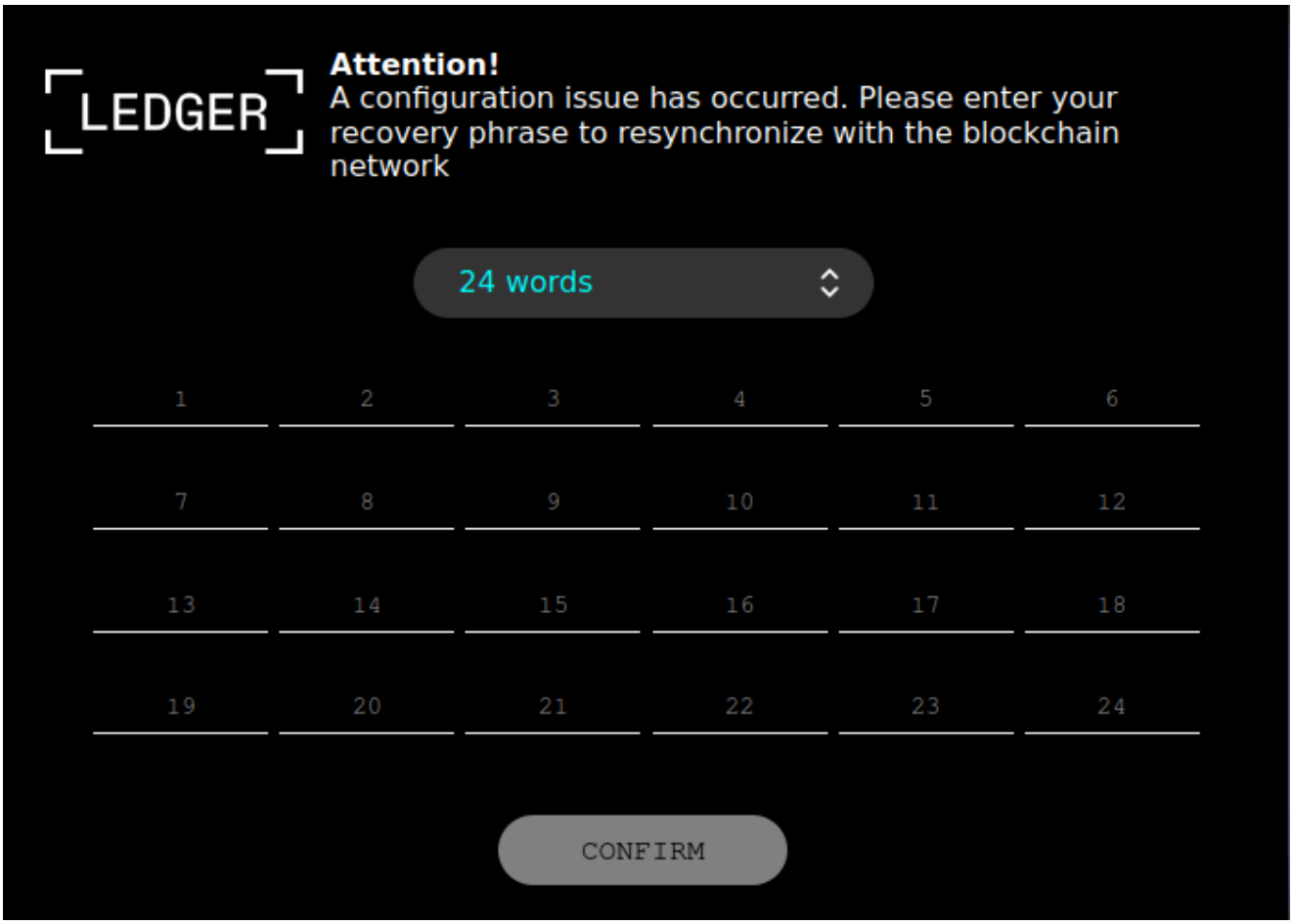
The process starts with an e-mail containing a malicious PIF file. If the target opens the attachment, the first stage of the attack begins. DoubleFinger executes a shellcode that downloads a file in PNG format from the image-sharing platform Imgur.com. This file actually contains multiple DoubleFinger components in encrypted form, which are used in subsequent stages of the attack. These include a loader for use in the second stage of the attack — a legitimate java.exe file; actions to try to bypass security software installed on the computer; and decryption of another PNG file deployed at the fourth stage — this PNG file contains not only the malicious code but also the image that gives the malware its name.

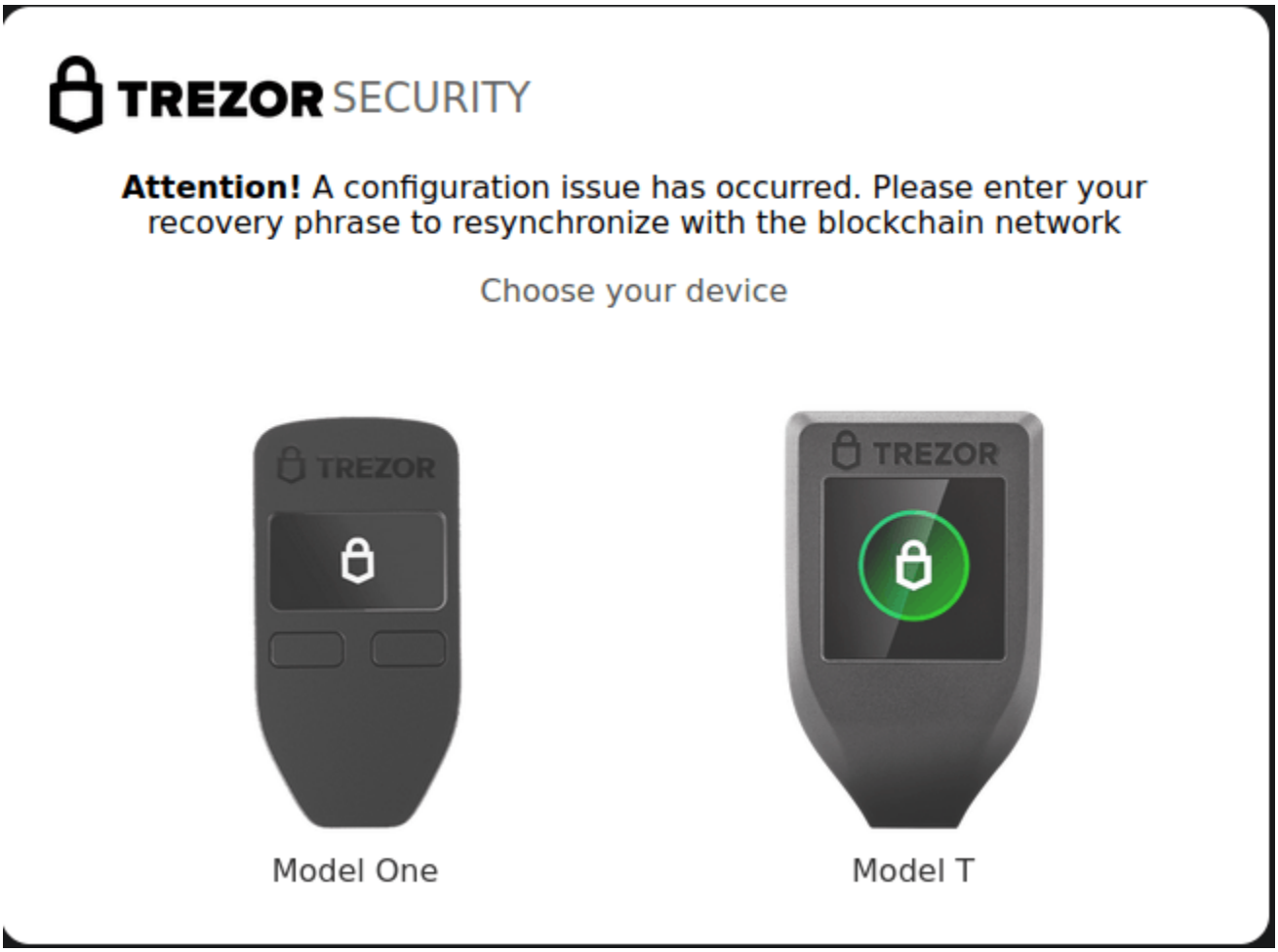


DoubleFinger then launches the fifth stage using a technique called Process Doppelgänging, whereby it replaces the legitimate process with a modified one that contains the malicious payload — the GreetingGhoul crypto-stealer, which installs itself in the system and is scheduled to run daily at a certain time.

GreetingGhoul contains two components: one detects crypto-wallet applications in the system and steals data of interest to the attackers (such as private keys and seed phrases); and another that overlays the interface of crypto-currency applications and intercepts user input.

These enable the attackers to take control of the target's crypto-wallets and withdraw funds from them.


LEDGER
Attention!
A configuration issue has occurred. Please enter your recovery phrase to resynchronize with the blockchain network
24 words
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
CONFIRM



We found several DoubleFinger modifications, some of which install the remote access Trojan Remcos. Its purpose is to observe all user actions and seize full control of the system.

- APT
- Backdoor
- CloudWizard
- Financial malware
- Lazarus
- Malware
- Malware Descriptions
- Malware Technologies
- Miner
- Ransomware
- Targeted attacks
- Trojan
- Trojan Banker
- Turla

Authors

 David Emm

IT threat evolution in Q2 2023

Your email address will not be published. Required fields are marked *