# IT threat evolution Q3 2021 - RedPacket Security

By April 2, 2026

Published: 2021-11-27 · Archived: 2026-04-05 15:01:10 UTC



## Targeted attacks

### WildPressure targets macOS

Last March, we reported a WildPressure campaign targeting industrial-related entities in the Middle East. While tracking this threat actor in spring 2021, we discovered a newer version. It contains the C++ Milum Trojan, a corresponding VBScript variant and a set of modules that include an orchestrator and three plugins. This confirms our previous assumption that there were more last-stagers besides the C++ ones.

Another language used by WildPressure is Python. The PyInstaller module for Windows contains a script named “Guard”. Interestingly, this malware was developed for both Windows and macOS operating systems. The coding style, overall design and C2 communication protocol is quite recognizable across all three programming languages used by the authors.

WildPressure used both virtual private servers (VPS) and compromised servers in its infrastructure, most of which were WordPress websites.

We have very limited visibility for the samples described in our report, but our telemetry suggests that the targets in this campaign were also from the oil and gas industry.

You can view our report on the new version here, together with a video presentation of our findings.

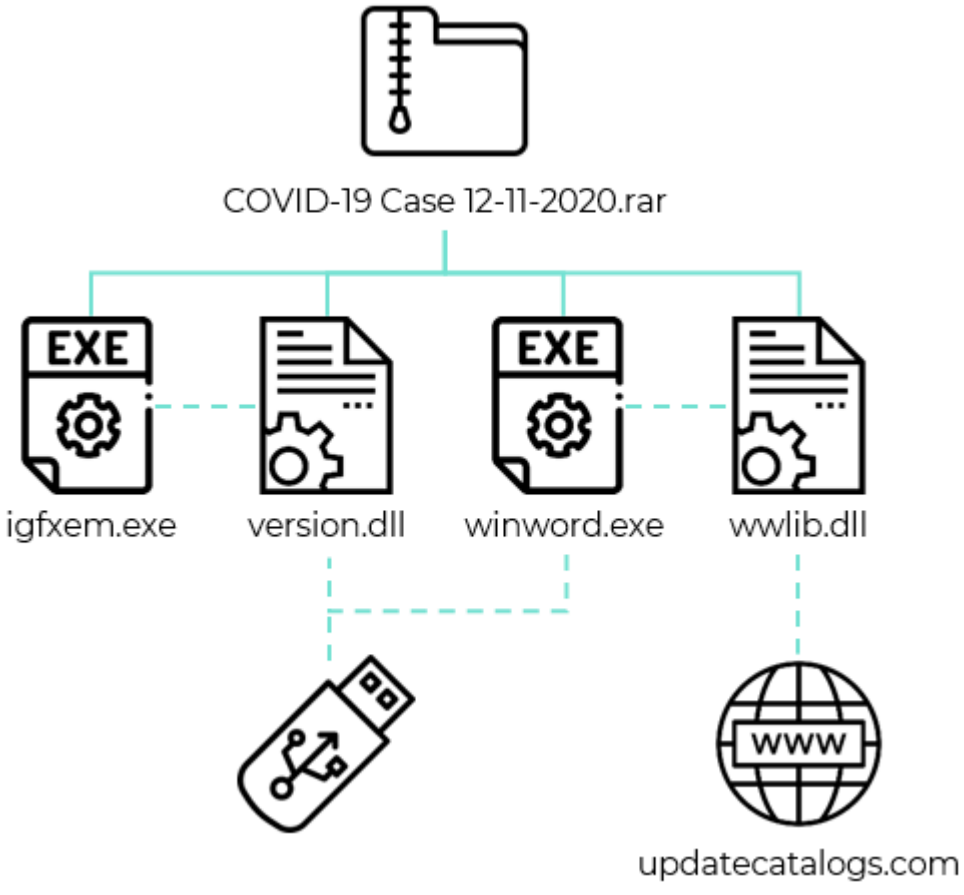
### LuminousMoth: sweeping attacks for the chosen few

We recently uncovered a large-scale and highly active attack against targets in Southeast Asia by a threat actor that we call LuminousMoth. The campaign dates back to October last year and was still ongoing at the time we published our public report in July. Most of the early sightings were in Myanmar, but it seems the threat actor is now much more active in the Philippines. Targets include high-profile organizations: namely, government entities located both within those countries and abroad.

Most APT threats carefully select their targets and tailor the infection vectors, implants and payloads to the victims' identities or environment. It's not often we observe a large-scale attack by APT threat actors – they usually avoid such attacks because they are too 'noisy' and risk drawing attention to the campaign. LuminousMoth is an exception. We observed a high number of infections; although we think the campaign was aimed at a few targets of interest.

The attackers obtain initial access to a system by sending a spear-phishing email to the victim containing a Dropbox download link. The link leads to a RAR archive that masquerades as a Word document. The archive contains two malicious DLL libraries as well as two legitimate executables that side-load the DLL files. We found multiple archives like this with file names of government entities linked to Myanmar.

We also observed a second infection vector that comes into play after the first one has successfully finished. The malware tries to spread to other hosts on the network by infecting USB drives.



In addition to the malicious DLLs, the attackers also deployed a signed, but fake version of the popular application Zoom on some infected systems, enabling them to exfiltrate data.

The threat actor also deploys an additional tool that accesses a victim's Gmail session by stealing cookies from the Chrome browser.

Infrastructure ties as well as shared TTPs allude to a possible connection between LuminousMoth and the HoneyMyte threat group, which has been seen targeting the same region using similar tools in the past.

### Targeted attacks exploiting CVE-2021-40444

On September 7, Microsoft reported a zero-day vulnerability (CVE-2021-40444) that could allow an attacker to execute code remotely on vulnerable computers. The vulnerability is in MSHTML, the Internet Explorer engine. Even though few people use IE nowadays, some programs use its engine to handle web content – in particular, Microsoft Office applications.

We have seen targeted attacks exploiting the vulnerability to target companies in research and development, the energy sector and other major industries, banking, the medical technology sector, as well as telecoms and IT.

To exploit the vulnerability, attackers embed a special object in a Microsoft Office document containing a URL for a malicious script. If the victim opens the document, Microsoft Office downloads the script and runs it using the MSHTML engine. Then the script can use ActiveX controls to perform malicious actions on the victim's computer.

### Tomiris backdoor linked to SolarWinds attack

The SolarWinds incident last December stood out because of the extreme carefulness of the attackers and the high-profile nature of their victims. The evidence suggests that the threat actor behind the attack, DarkHalo (aka Nobelium), had spent six months inside OrionIT's networks to perfect their attack. The following timeline sums up the different steps of the campaign.

In June, more than six months after DarkHalo had gone dark, we observed the DNS hijacking of multiple government zones of a CIS member state that allowed the attacker to redirect traffic from government mail servers to computers under their control – probably achieved by obtaining credentials to the control panel of the victims' registrar. When victims tried to access their corporate mail, they were redirected to a fake copy of the web interface.

After this, they were tricked into downloading previously unknown malware. The backdoor, dubbed Tomiris, bears a number of similarities to the second-stage malware, Sunshuttle (aka GoldMax), used by DarkHalo last year. However, there are also a number of overlaps between Tomiris and Kazuar, a backdoor that has been linked to the Turla APT threat actor. None of the similarities is enough to link Tomiris and Sunshuttle with sufficient confidence. However, taken together they suggest the possibility of common authorship or shared development practices.

You can read our analysis here.

### GhostEmperor

Earlier this year, while investigating the rise of attacks against Exchange servers, we noticed a recurring cluster of activity that appeared in several distinct compromised networks. We attribute the activity to a previously unknown

threat actor that we have called GhostEmperor. This cluster stood out because it used a formerly unknown Windows kernel mode rootkit that we dubbed Demodex; and a sophisticated multi-stage malware framework aimed at providing remote control over the attacked servers.

The rootkit is used to hide the user mode malware's artefacts from investigators and security solutions, while demonstrating an interesting loading scheme involving the kernel mode component of an open-source project named Cheat Engine to bypass the Windows Driver Signature Enforcement mechanism.

We identified multiple attack vectors that triggered an infection chain leading to the execution of the malware in memory. The majority of GhostEmperor infections were deployed on public-facing servers, as many of the malicious artefacts were installed by the httpd.exe Apache server process, the w3wp.exe IIS Windows server process, or the oc4j.jar Oracle server process. This means that the attackers probably abused vulnerabilities in the web applications running on those systems, allowing them to drop and execute their files.

Although infections often start with a BAT file, in some cases the known infection chain was preceded by an earlier stage: a malicious DLL that was side-loaded by wdichost.exe, a legitimate Microsoft command line utility (originally called MpCmdRun.exe). The side-loaded DLL then proceeds to decode and load an additional executable called license.rtf. Unfortunately, we did not manage to retrieve this executable, but we saw that the consecutive actions of loading it included the creation and execution of GhostEmperor scripts by wdichost.exe.

This toolset was in use from as early as July 2020, mainly targeting Southeast Asian entities, including government agencies and telecoms companies.

### FinSpy: analysis of current capabilities

At the end of September, at the Kaspersky Security Analyst Summit, our researchers provided an overview of FinSpy, an infamous surveillance toolset that several NGOs have repeatedly reported being used against

journalists, political dissidents and human rights activists. Our analysis included not only the Windows version of FinSpy, but also Linux and macOS versions, which share the same internal structure and features.

After 2018, we observed falling detection rates for FinSpy for Windows. However, it never actually went away – it was simply using various first-stage implants to hide its activities. We started detecting some suspicious backdoored installer packages (including TeamViewer, VLC Media Player and WinRAR); then in the middle of 2019 we found a host that served these installers along with FinSpy Mobile implants for Android.

The authors have gone to great lengths to make FinSpy inaccessible to security researchers – it seems they have put as much work into anti-analysis and obfuscation as they have into the Trojan itself. First, the samples are protected with multiple layers of evasion tactics.

Moreover, once the Trojan has been installed, it is heavily camouflaged using four complex, custom-made obfuscators.

Apart from Trojanized installers, we also observed infections involving use of a UEFI (Unified Extensible Firmware Interface) and MBR (Master Boot Record) bootkit. While the MBR infection has been known since at least 2014, details on the UEFI bootkit were publicly revealed for the first time in our private report on FinSpy.

The user of a smartphone or tablet can be infected through a link in a text message. In some cases (for example, if the victim's iPhone has not been not jailbroken), the attacker may need physical access to the device.

## Other malware

### REvil attack on MSPs and their customers worldwide

An attack perpetrated by the REvil Ransomware-as-a-Service gang (aka Sodinokibi) targeting Managed Service Providers (MSPs) and their clients was discovered on July 2.

The attackers identified and exploited a zero-day vulnerability in the Kaseya Virtual System/Server Administrator (VSA) platform. The VSA software, used by Kaseya customers to remotely monitor and manage software and network infrastructure, is supplied either as a cloud service or via on-premises VSA servers.

The exploit involved deploying a malicious dropper via a PowerShell script. The script disabled Microsoft Defender features and then used the certutil.exe utility to decode a malicious executable (agent.exe) that dropped an older version of Microsoft Defender, along with the REvil ransomware packed into a malicious library. That library was then loaded by the legitimate MsMpEng.exe by utilizing the DLL side-loading technique.

The attack is estimated to have resulted in the encryption of files belonging to around 60 Kaseya customers using the on-premises version of the platform. Many of them were MSPs who use VSA to manage the networks of other businesses. This MSP connection gave REvil access to those businesses, and Kaseya estimated that around 1,500 downstream businesses were affected.

Using our Threat Intelligence service, we observed more than 5,000 attack attempts in 22 countries by the time our analysis of the attack was published.

## What a [Print]Nightmare

Early in July, Microsoft published an alert about vulnerabilities in the Windows Print Spooler service. The vulnerabilities, CVE-2021-1675 and CVE-2021-34527 (aka PrintNightmare), can be used by an attacker with a regular user account to take control of a vulnerable server or client machine that runs the Windows Print Spooler

service. This service is enabled by default on all Windows clients and servers, including domain controllers, making both vulnerabilities potentially very dangerous.

Moreover, owing to a misunderstanding between teams of researchers, a proof-of-concept (PoC) exploit for PrintNightmare was published online. The researchers involved believed that Microsoft's Patch Tuesday release in June had already solved the problem, so they shared their work with the expert community. However, while Microsoft had published a patch for CVE-2021-1675, the PrintNightmare vulnerability remained unpatched until July. The PoC was quickly removed, but not before it had been copied multiple times.

CVE-2021-1675 is a privilege elevation vulnerability, allowing an attacker with low access privileges to craft and use a malicious DLL file to run an exploit and gain higher privileges. However, that is only possible if the attacker already has direct access to the vulnerable computer in question.

CVE-2021-34527 is significantly more dangerous because it is a remote code execution (RCE) vulnerability, which means it allows remote injection of DLLs.

You can find a more detailed technical description of both vulnerabilities here.

## Grandoreiro and Melcoz arrests

In July, the Spanish Ministry of the Interior announced the arrest of 16 people connected to the Grandoreiro and Melcoz (aka Mekotio) cybercrime groups. Both groups are originally from Brazil and form part of the Tetrade umbrella, operating for a few years now in Latin America and Western Europe.

The Grandoreiro banking Trojan malware family initially started its operations in Brazil and then expanded its operations to other Latin American countries and then to Western Europe. The group has regularly improved its techniques; and, based on our analysis of the group's campaigns, it operates as a malware-as-a-service (MaaS) project. Our telemetry shows that, since January 2020, Grandoreiro has mainly attacked victims in Brazil, Mexico, Spain, Portugal and Turkey.

Melcoz had been active in Brazil since at least 2018, before expanding overseas. We observed the group attacking assets in Chile in 2018 and, more recently, in Mexico: it's likely that there are victims in other countries too, as some of the targeted banks have international operations. As a rule, the malware uses AutoIt or VBS scripts, added into MSI files, which run malicious DLLs using the DLL-Hijack technique, aiming to bypass security solutions. The malware steals passwords from browsers and from the device's memory, providing remote access to capture internet banking access. It also includes a Bitcoin wallet stealing module. Our telemetry confirms that, since January 2020, Melcoz has been actively targeting Brazil, Chile and Spain, among other countries.

Since both malware families are from Brazil, the individuals arrested in Spain are just operators. So, it's likely that the creators of Grandoreiro and Melcoz will continue to develop new malware techniques and recruit new members in their countries of interest.

## Gamers beware

Earlier this year, we discovered an ad in an underground forum for a piece of malware dubbed BloodyStealer by its creators. The malware is designed to steal passwords, cookies, bank card details, browser auto-fill data, device information, screenshots, desktop and client uTorrent files, Bethesda, Epic Games, GOG, Origin, Steam, Telegram, and VimeWorld client sessions and logs.

***The BloodyStealer ad (Source: https://twitter.com/3xp0rtblog)***

The authors of the malware, which has hit users in Europe, Latin America and the Asia-Pacific region, have adopted a MaaS distribution model, meaning that anyone can buy it for the modest price of around $10 per month (roughly $40 for a “lifetime license”).

On top of its theft functions, the malware includes tools to thwart analysis. It sends stolen information as a ZIP archive to the C2 (command-and-control) server, which is protected against DDoS (distributed denial of service) attacks. The cybercriminals use either the (quite basic) control panel or Telegram to obtain the data, including gamer accounts.

BloodyStealer is just one of many tools available on the dark web for stealing gamer accounts. Moreover, underground forums often feature ads offering to post a malicious link on a popular website or selling tools to

generate phishing pages automatically. Using these tools, cybercriminals can collect, and then try to monetize, a huge amount of credentials. All kinds of offers related to gamer accounts can be found on the dark web.

So-called logs are among the most popular. These are databases containing reams of data for logging into accounts. In their ads, attackers can specify the types of data, the geography of users, the period over which the logs were collected and other details. For example, in the screenshot below, an underground forum member offers an archive with 65,600 records, of which 9,000 are linked to users from the US, and 5,000 to residents of India, Turkey and Canada. The entire archive costs $150 (that’s about 0.2 cents per record).

Cybercriminals can also use compromised gaming accounts to launder money, distribute phishing links and conduct other illegal business.

You can read more about gaming threats, including BloodyStealer, here and here.

## Triada Trojan in WhatsApp mod

Not everyone is happy with the official WhatsApp app, turning instead to modified WhatsApp clients for features that the WhatsApp developers haven't yet implemented in the official version. The creators of these mods often embed ads in them. However, their use of third-party ad modules can provide a mechanism for malicious code to be slipped into the app unnoticed.

This happened recently with FMWhatsApp, a popular WhatsApp mod. In version 16.80.0 the developers used a third-party ad module that includes the Triada Trojan (detected by Kaspersky's mobile antivirus as

Trojan.AndroidOS.Triada.ef). This Trojan performs an intermediary function. First, it collects data about the user's device, and then, depending on the information, it downloads one of several other Trojans. You can find a description of the functions that these other Trojans perform in our analysis of the infected FMWhatsApp mod.

## Qakbot banking Trojan

QakBot (aka QBot, QuackBot and Pinkslipbot) is a banking Trojan that was first discovered in 2007, and has been continually maintained and developed since then. It is now one of the leading banking Trojans around the globe. Its main purpose is to steal banking credentials (e.g., logins, passwords, etc.), but it has also acquired functionality allowing it to spy on financial operations, spread itself and install ransomware in order to maximize revenue from compromised organizations.

The Trojan also includes the ability to log keystrokes, backdoor functionality, and techniques to evade detection. The latter includes virtual environment detection, regular self-updates and cryptor/packer changes. QakBot also tries to protect itself from being analyzed and debugged by experts and automated tools. Another interesting piece of functionality is the ability to steal emails: these are later used by the attackers to send targeted emails to the victims, with the information obtained used to lure victims into opening those emails.

QakBot is known to infect its victims mainly via spam campaigns. In some cases, the emails are delivered with Microsoft Office documents or password-protected archives with documents attached. The documents contain macros and victims are prompted to open the attachments with claims that they contain important information (e.g., an invoice). In some cases, the emails contain links to web pages distributing malicious documents.

However, there is another infection vector that involves a malicious QakBot payload being transferred to the victim's machine via other malware on the compromised machine. The initial infection vectors may vary depending on what the threat actors believe has the best chance of success for the targeted organization(s). It's known that various threat actors perform reconnaissance of target organizations beforehand to decide which infection vector is most suitable.

We analyzed statistics on QakBot attacks collected from our Kaspersky Security Network (KSN), where anonymized data voluntarily provided by Kaspersky users is accumulated and processed. In the first seven months of 2021 our products detected 181,869 attempts to download or run QakBot. This number is lower than the detection number from January to July 2020, though the number of users affected grew by 65% – from 10,493 in the previous year to 17,316 this year.

*Number of users affected by QakBot attacks from January to July in 2020 and 2021 (download)*

You can read our full analysis here.

If you like the site, please consider joining the telegram channel or supporting us on Patreon using the button below.

---

Source: https://www.redpacketsecurity.com/it-threat-evolution-q3-2021/