2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

GOODBYE LOADERS, HELLO RMM: THE RISE OF LEGIT SOFTWARE IN ECRIME CAMPAIGNS

Ole Villadsen & Selena Larson

Proofpoint, USA

selenalarson@gmail.com
ovilladsen@proofpoint.com

ABSTRACT

Cybercriminals are increasingly using legitimate remote access software as an initial access method to deliver malware. Historically, threat actors delivering malware, including ransomware, used remote access software and remote monitoring and management (RMM) tools as part of an overall attack chain, typically once a host was already compromised. Now, tools like *ScreenConnect*, *Atera* and *Bluetrait* are often observed as the first step in an attack chain, delivered directly via phishing emails.

In this paper we will discuss:

- Why and how the cybercrime initial access landscape has drastically shifted
- What are the most frequentlyw observed RMM payloads
- How new techniques can bypass existing detections and how defenders can respond

The information detailed in this report was gathered up to June 2025.

INTRODUCTION

Cybercriminals are increasingly turning to remote monitoring and management (RMM) tools as a first-stage payload in email threat campaigns. Sometimes referred to as remote access software (RAS), these tools are used throughout enterprises to remotely manage fleets of computers. When abused, RMMs can act like remote access trojans (RATs), enabling reconnaissance, data theft, lateral movement, and can be used to deploy additional payloads like ransomware.

RMMs have been a staple of cybercriminal activity for years, typically observed as part of an attack chain once a threat actor had already gained access to a target system. For example, ransomware threat actors and affiliates either use software vulnerabilities or stolen credentials to gain access to existing RMM tooling in a compromised environment or download such software themselves to enable lateral movement and remote access. Examples include LAPSUS$ [1] (*RealVNC*, *AnyDesk*, *LogMeIn*, *TeamViewer*) and Black Basta [2] (*Splashtop*, *ScreenConnect*). And this is still quite a common technique. Additionally, threat actors conducting telephone-oriented attack delivery (TOAD) campaigns [3], that lure a person into calling a fake helpdesk, have also used RMMs for years. In this case, it is an initial access payload but deployed only after someone calls the threat actor and engages directly with them, and the user downloads it themselves.

Recently, however, ecrime threat actors have begun adopting RMM tools as a first-stage payload delivered via email campaigns. That is, instead of delivering a RAT or malware loader, they send RMM payloads via attachments or URLs. This is a distinct shift in the ecrime threat landscape observed since mid-2024. We also observe espionage threat actors distributing RMM/RAS tooling as a first-stage payload, but this report focuses on their use in cybercrime campaigns, which has seen substantial growth.

WHY RMM?

Proofpoint currently tracks multiple threat clusters distributing RMM tooling, and the number of unique RMMs observed in threat data, as well as the number of threat actors using them, continues to increase in campaign data. We track actors and malware via campaigns. A campaign is defined by *Proofpoint* as a timebound set of related threat activity analysed by our researchers. Notably, while *NetSupport* had historically been the most frequently observed RMM in our campaign data, its use dropped off throughout 2024 and other RMMs became much more prominent. This trend is continuing in 2025. (Note: *Proofpoint* implemented new RMM detections beginning in 2024, so it is possible that increased visibility also contributed to an increase in observed campaigns, and the use of obscure or less popular RMM software may not be as present in campaign data before this time.)

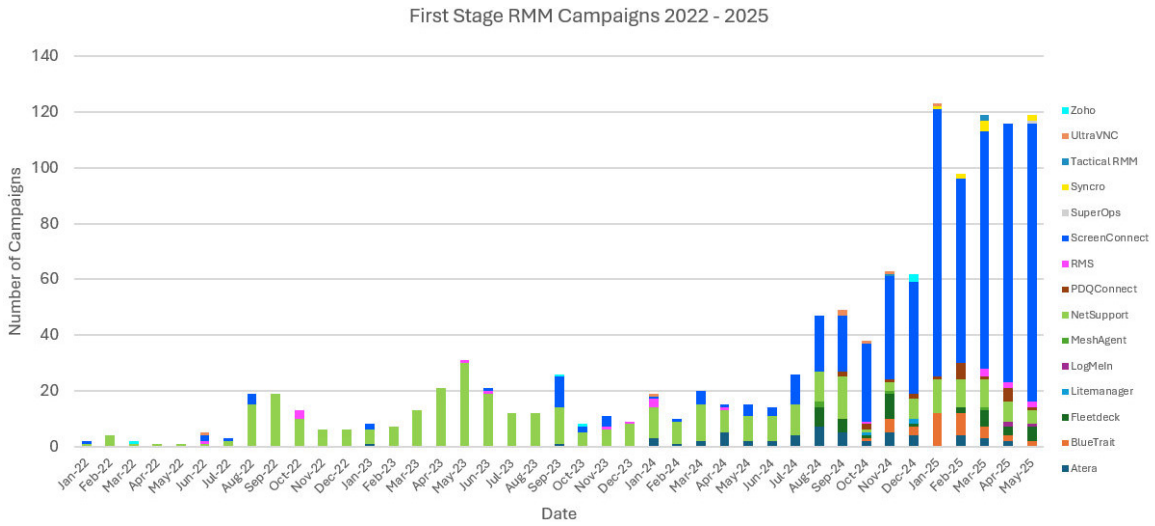


Figure 1: RMMs/RAS observed in Proofpoint data.

The spike in this type of software aligns with the decrease in malware loaders that criminal initial access brokers (IABs) relied on for years. We have seen a drastic decrease in the number of loaders and botnets delivered via email as a first-stage payload. There are likely multiple reasons for this. Detection and defence against loaders and malware in general has improved, so threat actors have had to change their tactics, techniques and procedures (TTPs). For example, *Microsoft* disabling macros by default in 2022 [4] caused a significant shift in payloads and attack chains, with actors trying to figure out new tricks to achieve the same level of success as the reliable 'click to enable macros' technique. Law enforcement disruptions including those associated with Operation Endgame [5] also imposed cost on threat actors and removed reliable malware providers, forcing threat actors to find other tooling. And in general across the landscape, there is increasing focus on exploiting identity via information stealers and credential phishing.

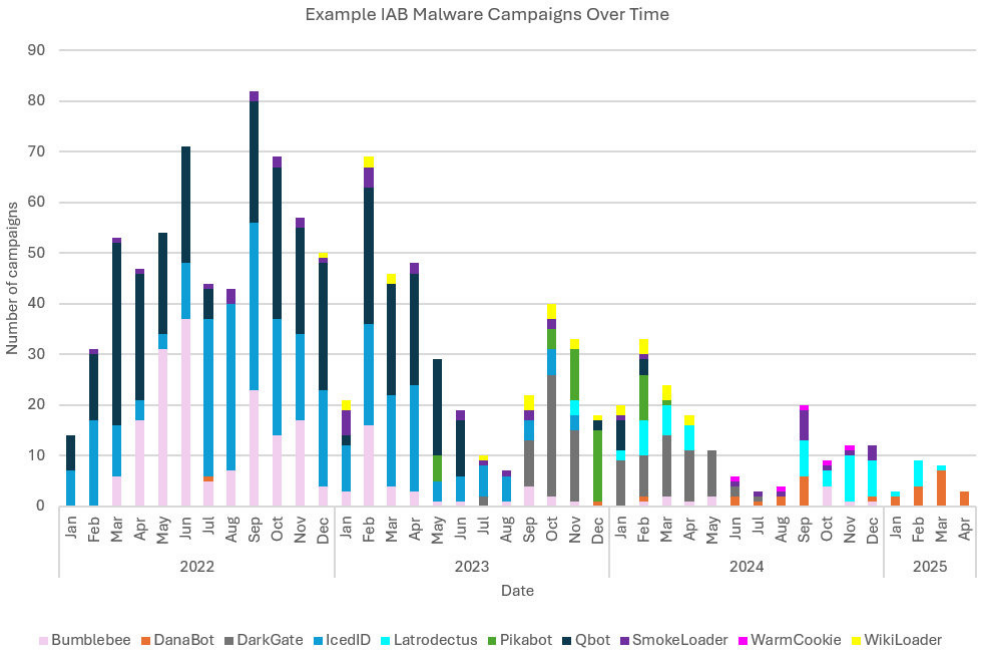
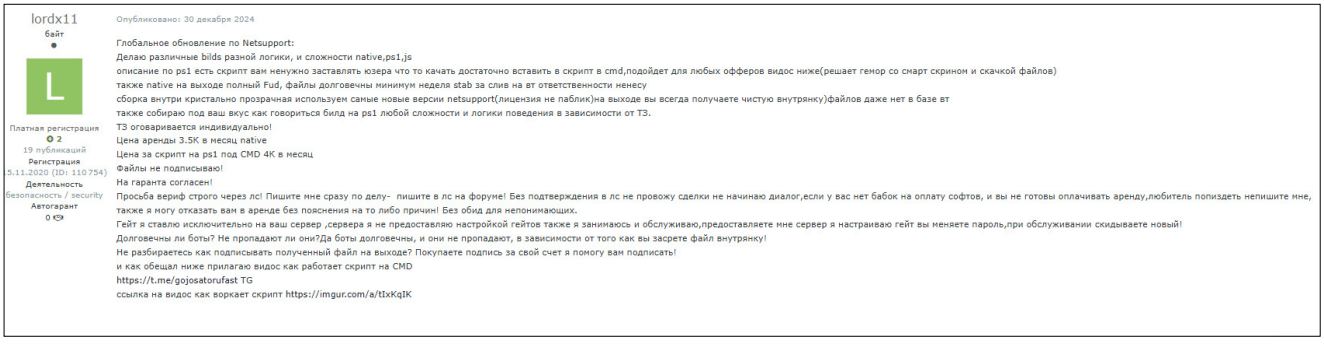


Figure 2: Example major IAB malware families observed in email threat data.

Threat actors can buy access to RMM services directly from vendor websites or on various criminal forums in much the same way as purchasing access to loaders, information stealers, or any other malware. The benefit of using 'legitimate' software as a first-stage payload is that it can masquerade as legitimate traffic. If organizations are not monitoring and detecting rogue RMM software within their environments, criminal activity may just look like enterprise software. Threat actors can register accounts to use the software via cloud-based installations that connect to the providers' servers directly, or set up or purchase self-hosted (or criminally-hosted) on-prem installations.

We have observed multiple forum posts advertising access to RMMs including *NetSupport* and *ScreenConnect*.


lordx11
байт
L
Платная регистрация
2
19 публикаций
Регистрация
5.11.2020 (ID: 110 754)
Деятельность
безопасность / security
Автогарант
0

Опубликовано: 30 декабря 2024

Глобальное обновление по Netsupport:
Делаю различные bilds разной логики, и сложности native,ps1,js
описание по ps1 есть скрипт вам ненужно заставлять юзера что то качать достаточно вставить в скрипт в cmd,подойдет для любых офферов видос ниже(решает генор со смарт скрином и скачкой файлов)
также native на выходе полный Fud, файлы долговечны минимум неделя stab за слив на вт ответственности ненесу
сборка внутри кристально прозрачная используем самые новые версии netsupport(лицензия не паблик)на выходе вы всегда получаете чистую внутрянку)файлов даже нет в базе вт
также собираю под ваш вкус как говориться билд на ps1 любой сложности и логики поведения в зависимости от ТЗ.
ТЗ оговаривается индивидуально!
Цена аренды 3.5К в месяц native
Цена за скрипт на ps1 под CMD 4К в месяц
Файлы не подписываю!
На гаранта согласен!
Просьба вериф строго через лс! Пишите мне сразу по делу- пишите в лс на форуме! Без подтверждения в лс не провожу сделки не начинаю диалог,если у вас нет бабок на оплату софтов, и вы не готовы оплачивать аренду,любитель попиздеть непишите мне, также я могу отказать вам в аренде без пояснения на то либо причин! Без обид для непонимающих.
Гейт я ставлю исключительно на ваш сервер ,сервера я не предоставляю настройкой гейтов также я занимаюсь и обслуживаю,предоставляете мне сервер я настраиваю гейт вы меняете пароль,при обслуживании скидываете новый!
Долговечны ли боты? Не пропадают ли они?Да боты долговечны, и они не пропадают, в зависимости от того как вы засрете файл внутрянку!
Не разбираетесь как подписывать полученный файл на выходе? Покупаете подпись за свой счет я помогу вам подписать!
и как обещал ниже прилагаю видос как работает скрипт на CMD
https://t.me/gojosatorufast TG
ссылка на видос как воркает скрипт https://imgur.com/a/tIxKqIK

Figure 3: Advertisement on a criminal forum selling access to NetSupport builds for $3,500 per month.

According to data shared with *Proofpoint* from intelligence firm *Qintel*, beginning in late 2024, multiple actors began offering access to RMM software setups as a service on a variety of forums including BreachForums, xss, and Exploit. Monthly subscription prices ranged from $250 for cloud-based services to up to $6,000 for on-prem hosted services for multiple users. At least one zero-day was offered for sale for an unnamed RMM, costing $60,000. *Qintel* researchers also observed multiple threads on criminal forums seeking feedback on the 'best' RMM, and software referenced included *MeshCentral*, *SplashTop*, *AnyDesk*, *TeamViewer*, *Atera*, *GetScreen*, *ScreenConnect* and *Tactical RMM*. In addition to

selling, some actors are also seeking. One actor, for example, posted ads suspected to be for ransomware affiliates who could work with RMM software: 'We need top networkers who know how to bypass problematic AB like sentinel, work with RMM (Remote Monitoring Management) and EDR and backups. Your skills will pay off handsomely! The current rate is 80/20.'

Social engineering to RMM infections

One other notable trend in the cybercriminal threat landscape is leveraging targeted social engineering over the phone or messaging apps, such as telephone-oriented attack delivery (TOAD) attacks [3], or voice phishing (vishing). This can lead to people verbally engaging directly with threat actors and following instructions to install legitimate remote access tools. In many cases, this can lead to ransomware.

For example, beginning in 2024, threat actors distributing Black Basta ransomware began using a unique social engineering attack chain. The campaigns began with 'email bombing' or sending 'legitimate' mail to overwhelm a target's inbox. Then, the actors impersonated IT employees in vishing attacks via phone or *Microsoft Teams* and convinced people [6] to grant access to the threat actors via *Quick Assist*, or to download *AnyDesk* [7]. Notably, threat actors delivering Black Basta previously used IAB malware compromises like Qbot or Pikabot for initial access. While *Microsoft* reported [6] that Qbot was used in the vishing attacks as part of an overall attack chain once access had been gained via remote access, the disruption of such loaders almost certainly forced the actors to retool and try new attack chains rather than delivering large volumes of email.

But phone-based social engineering leading to malware, although increasing in popularity, is not a new technique. For example, back in 2021 *Proofpoint* observed threat actors delivering BazaLoader via fake invoices [8] containing phone numbers, leveraging the TOAD technique to convince people to call to dispute charges. In this case, it led to malware directly, but now threat actors typically convince targets to install RMMs. For example, the Silent ransomware group sends fake subscription emails containing phone numbers to call to dispute charges, and once a target calls the phone number, they're directed to download and install an RMM for 'support'. When we engaged with a suspected Silent ransomware email and phone call, the threat actor directed our researcher to download *Zoho Assist*. However, the group has also been observed instructing targets [9] to download *Syncro*, *AnyDesk*, *Splashtop* or *Atera*.

TOAD attacks that lead to RMM installation are also very popular for business email compromise (BEC) threat actors and those conducting consumer-targeted fraud.

SUMMARY OF EMAIL CAMPAIGN DATA

We observe over a dozen unique RMM tools regularly in email threat data, and that number is increasing as threat actors expand to less well-known software. The open-source RMM tool repository LOLRMM [10] includes nearly 300 RMM or RAS applications that could be abused by adversaries.

While many of the campaigns are not attributed to a tracked threat actor, some of the most high-volume criminal threat actors incorporate these tools into their activities, including TA583 and TA2725.

Notable threat clusters

ScreenConnect and TA583

ScreenConnect is by far the most common RMM delivered via email. *Proofpoint* attributes most *ScreenConnect* campaigns to TA583, a highly active threat actor that conducts multiple campaigns each day using this RMM. The scale of these operations varies significantly, ranging from tens of thousands of messages to only a handful of emails in our telemetry.

TA583 is a cybercriminal threat actor with the goal of obtaining remote access in target environments. Once having gained access, the group has been observed using *ScreenConnect* to deploy AsyncRAT [11] and BrowserCredExtractor [12], a tool publicly available on *GitHub* to extract browser credentials.

Beyond credential theft, specific objectives once a system is compromised are outside of our visibility, but may include account take over (ATO), cryptocurrency theft, data exfiltration, and possibly brokering initial access for other threat actors. *Proofpoint* has tracked this actor since 2022 through email lures, targeting, malware payloads, and network infrastructure, but only designated a TA number in January 2025. Prior to mid-2024, TA583 mostly deployed AsyncRAT; however, since then the actor has primarily used *ScreenConnect* as an initial access payload.

Most observed campaigns deliver *ScreenConnect* using URLs, although many also deliver HTML, PDF, or SVG attachments. These URLs frequently use email shortener services and publicly available services such as *Canva*, *Dropbox*, *Amazon* and *Bitbucket*. TA583 most often uses lures related to the U.S. Social Security Administration. Other observed lures include the U.S. Internal Revenue Service, U.S. Postal Service (USPS), various telecommunications providers, and more.

For example, on 24 April 2025, we identified a campaign impersonating the U.S. Social Security Administration. Messages contained URLs leading to an executable, which, if executed, installed *ScreenConnect*.

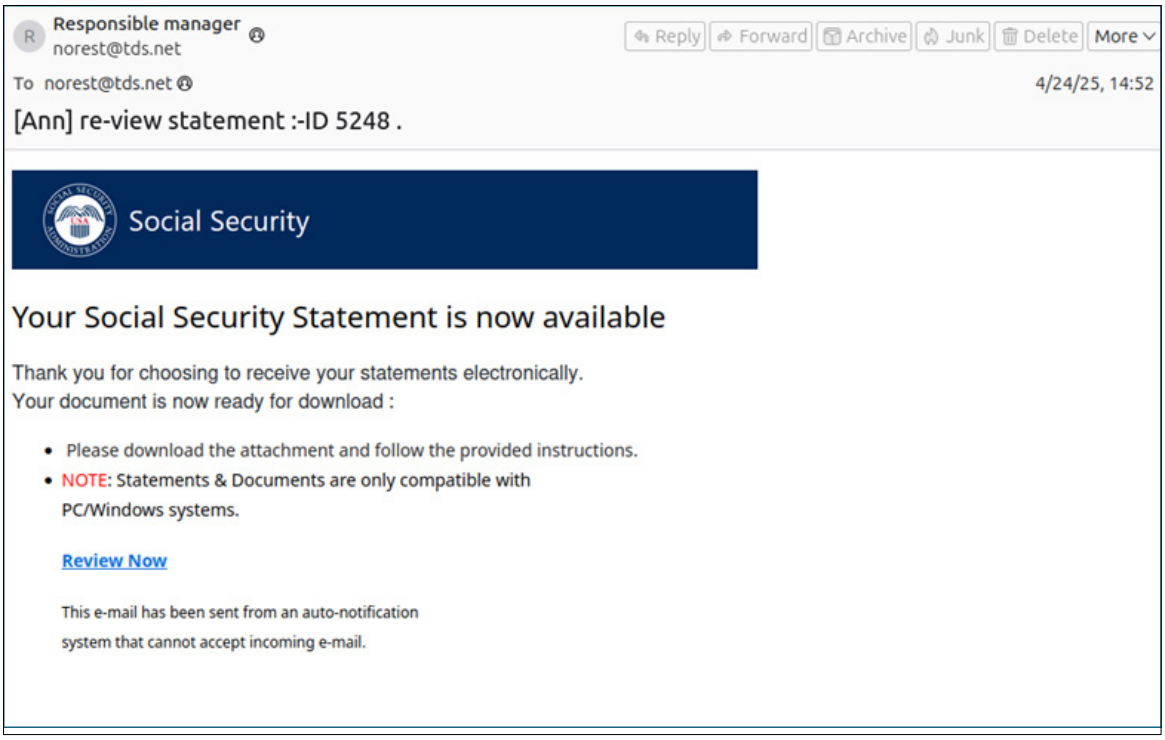


Figure 4: TA583 lure impersonating the U.S. Social Security Administration.

We often observe TA583 targeting free consumer email addresses provided by telecommunications providers. These accounts are frequently configured to automatically forward messages to users' corporate or educational email addresses. This behaviour introduces risk to organizations, particularly if recipients install *ScreenConnect* while using a work or school device.

We have observed TA583 commonly employ the following methods to deliver emails:

- Free consumer email accounts, including those provided by telecommunications providers
- Email marketing and survey platforms (e.g. *Sendgrid*, *Mailjet* and *Qualtrics*)
- Compromised email accounts.

Expansion of ScreenConnect activity in 2025

Since early January 2025, there has been a noteworthy increase in *ScreenConnect* campaigns. However, we cannot definitively attribute all these campaigns to TA583, as many employ lures, tactics, targeting or infrastructure that differ from those previously connected to the group. This evolution complicates attribution and suggests other threat activity clusters may also be delivering *ScreenConnect*.

That said, we have identified unusual overlaps between many *ScreenConnect* campaigns – including those that have not otherwise been definitively linked to TA583 – such as similarities in file names, domain names, hosting infrastructure, and the graphics and text used in *ScreenConnect* staging sites.

These similarities may stem from the use of common resources or providers, such as the emergence of dark web vendors selling *ScreenConnect* access beginning in late 2024 (see above). The emergence of these vendors also coincides with the increase in *ScreenConnect* that we observed during 2025, suggesting the growth of a broader ecosystem supporting *ScreenConnect* campaigns. This ecosystem could also include sharing templates, infrastructure, files, targets, and tactics among cybercriminals on underground forums and networks.

For example, one new tactic that we have observed in 2025 is a 'daisy chain' approach, where the threat actor uses *ScreenConnect* to access a user's email account and then sends malicious emails to the user's contacts. This technique increases the likelihood of compromise, as recipients are more likely to trust emails from known senders. For example, in May 2025, a user received an email from a compromised contact containing a link leading to *ScreenConnect*. After the user installed the tool, their email account was used the next day to send malicious emails to their own contacts.

We have also observed a notable increase in the use of new lures, including those in which the threat actor delivers an email lure with a link to a party invitation or a document of some sort that they wish to share with the recipient. Such attacks are often used in conjunction with the daisy chain method described above using compromised email accounts.

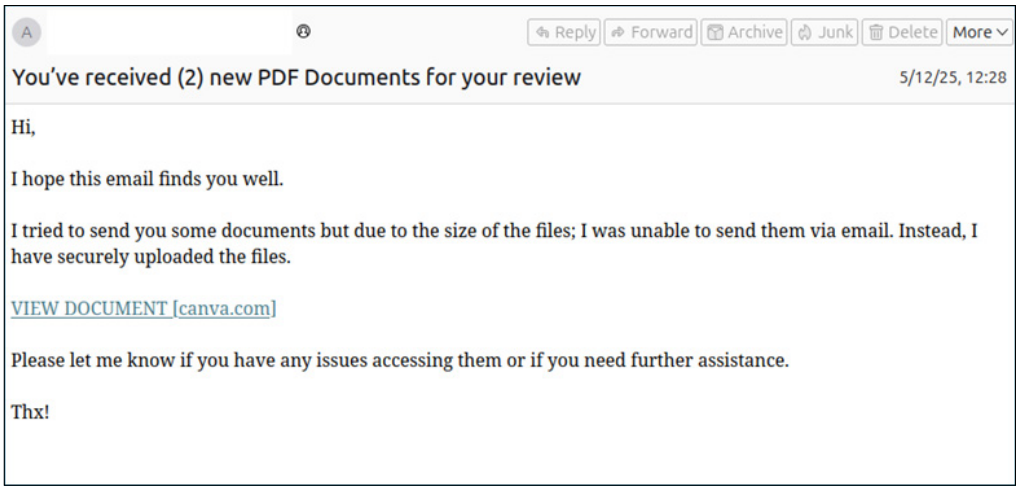


Figure 5: Email using compromised accounts to share an unspecified document that installs ScreenConnect.

UAC-0050: NetSupport and RMS

UAC-0050 [13] is another prominent threat actor that we have observed regularly delivering RMM tools, primarily *NetSupport* and *Remote Management System* (*RMS*). This threat actor has also targeted organizations in Ukraine with remote access trojans and information stealers such as Remcos and Lumma Stealer, respectively.

On 14 January 2025, *Proofpoint* researchers for the first time observed this actor deliver zipped PDFs with URLs leading to the installation of *NetSupport*. Since that time,we have observed UAC-0050 deliver *NetSupport* on at least 11 more occasions using the licensees: 'XMLCTL', 'DCVTTTUUEEW23', or 'EVALUSION'. In 2025, these campaigns typically deliver emails that contain *4Sync* or *Dropbox* URLs (or PDFs with those URLs) that lead to a JavaScript file which downloads and installs *NetSupport*.

In addition to *NetSupport*, we also observed UAC-0050 in early 2024 and throughout 2025 frequently deliver *Remote Management System* using these same techniques.

Notably, we have identified other threat actors that have also used those same *NetSupport* licensees, in particular a cluster of fake update campaigns leading to *NetSupport*. *Proofpoint* calls this activity ZPHP [14], and its activity is ongoing with weekly campaigns. The overlapping *NetSupport* configurations do not necessarily indicate that the activity is conducted by the same threat actor. It is possible there is a cracked or commercially available version of this payload.

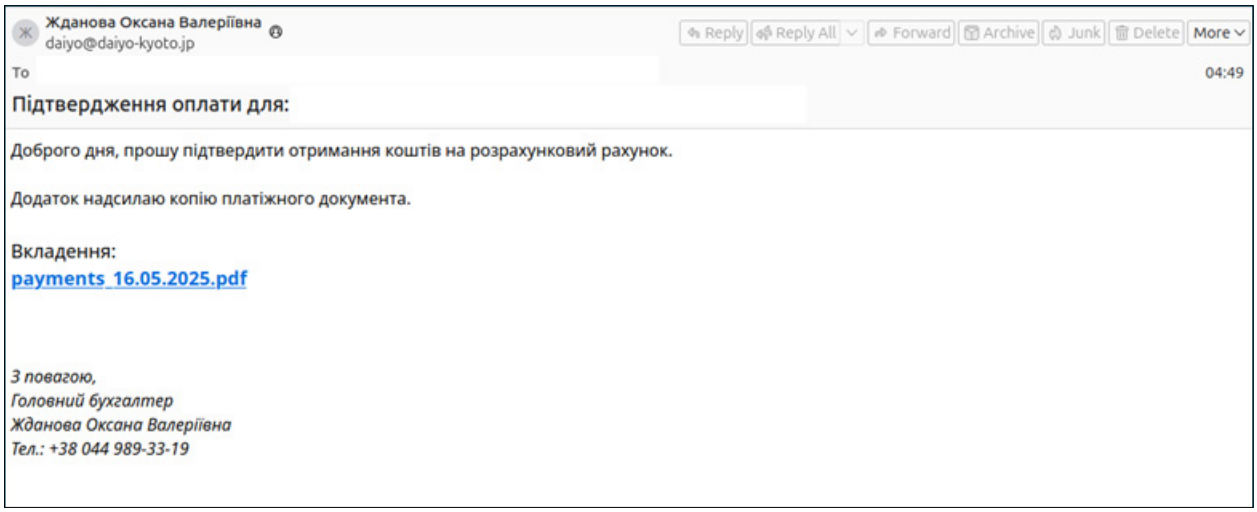


Figure 6: UAC-0050 campaign delivering RMS on 16 May 2025.

Fleetdeck and Bluetrait

Fleetdeck and *Bluetrait* are RMMs that are not frequently associated with cybercriminal activity; however, at least one activity cluster has used them regularly since August and October 2024, respectively.

Campaigns are typically low in volume, ranging from a handful to fewer than 500 messages per campaign. Messages are typically written in French, English or Spanish, and include payment-themed lures. On limited occasions in 2025, we also

observed this cluster deliver other RMMs, such as *SuperOps* and *Syncro*. The threat actor primarily uses PDFs with URLs leading to the *Fleetdeck* executable or *Bluetrait* MSI installer.

For example, we observed a campaign on 15 May 2025 using payment themes.

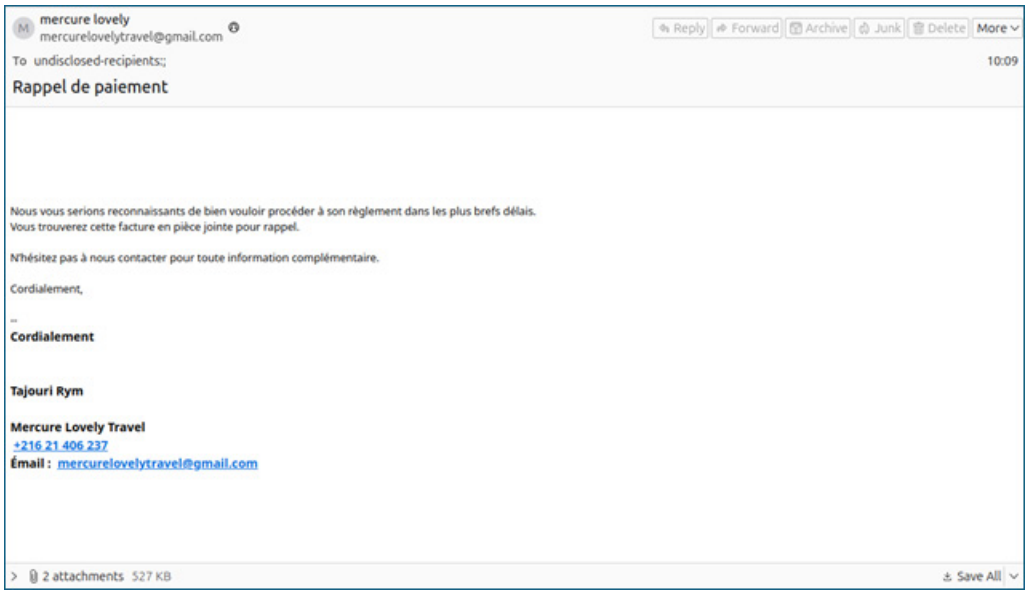


Figure 7: French language email distributing Fleetdeck and Syncro RMM.

In this campaign, the messages contain two PDFs with URLs: one leading to an executable file which installs *Fleetdeck*, and the other leading to an MSI file which installs *Syncro*.

We have also observed this activity cluster using *Bluetrait* to download and install additional RMMs/RAS, such as *ScreenConnect*, *Syncro* and *Tactical RMM*.

DETECTION AND DEFENCE

In general, *Proofpoint* recommends an allowlist approach to RMM/RAS. Organizations should block all traffic to domains that are not pre-approved by cybersecurity and information technology teams.

Detecting malicious use of legitimate RMMs can be difficult, especially as some threat actors use on-prem hosted versions as opposed to cloud. However, detecting C2 and combining that with behavioural and attack chain characteristics can provide a comprehensive view of the activity to contextualize malicious installations. At *Proofpoint*, for example, the key is to enrich an RMM identified in a sandbox with information from the email message, the attack chain, or known bad configurations from attackers that they previously used or that we know are cracked versions. So, the approach is: detect RMM (whether legitimate or not); extract the configuration; and condemn based on attack chain, email message, or known bad C2.

Proofpoint adds signatures for all new RMMs observed in our data – in many cases working off the LOLRMM database – in order to condemn them. Notably, we innovated with RMM detections in our sandbox, specifically around attack chain signatures. RMM campaigns were so unique that our detection engineers created a new capability to develop signatures looking at the entire attack chain to enable condemnation off various characteristics, simply because it's not appropriate to just block all RMMs as malware given their widespread legitimate use. *Proofpoint* is not sharing these details publicly, to prevent threat actors from innovating new evasion techniques.

Proofpoint Emerging Threats also maintains signatures for network traffic from legitimate RMM tools. Such alerts can detect both known malicious activity as well as generic traffic that may be unusual to see in an environment. These alerts, when fired in an organization, provide context for the observed traffic (domain, IP, C2, hash, etc.) for security teams to investigate. Many of these detections are based on campaigns observed in our threat data, with both ET PRO and ET OPEN signatures available for customers. In some cases, rules are designated as ET INFO to alert of potential suspicious activity but not block outright to potentially disrupt legitimate use in an environment. When such rules fire, it's important for the investigator to collect additional context such as the download link and initial access (like web inject, email, or phone call), to understand objectives before assuming a detection fired a false positive.

FUTURE ASSESSMENTS

Given the massive increase in popularity for RMM/RAS tooling, we anticipate that this will continue to be a favoured attack method for cybercriminal threat actors. Indeed, multiple members of our team have friends or family that have been targeted and infected with RMMs, indicating that the lure themes and attack chains can be very convincing.

Additionally, as law enforcement activities such as Operation Endgame continue to target malware loaders, botnets, and information stealers, threat actors will persist in adopting new TTPs, especially ones that have proven to be very effective, such is the case with RMMs.

We would like to thank *Qintel* and *DFIR Report* for collaborating on information sharing related to this activity.

REFERENCES

[1] Review of the attacks associated with LAPSUS$ and related threat groups. Cyber Safety Review Board. 24 July 2023. https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.

[2] #StopRansomware: Black Basta. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

[3] Larson S.; Scholten, S.; Kromphardt, T. Caught Beneath the Landline: A 411 on Call Center Scams. Proofpoint. 4 November 2021. https://www.proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery.

[4] Larson, S.; Wise, J. Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem. Proofpoint. 12 May 2023. https://www.proofpoint.com/us/blog/threat-insight/crime-finds-way-evolution-and-experimentation-cybercrime-ecosystem.

[5] Operation Endgame. https://operation-endgame.com/.

[6] Microsoft. Threat actors misusing Quick Assist in social engineering attacks leading to ransomware. 15 May 2024. https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/.

[7] Rapid7. Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators. 10 May 2024. https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/.

[8] Larson, S.; Mesa, M. BazaFlix: BazaLoader Fakes Movie Streaming Service. Proofpoint. 26 May 2021. https://www.proofpoint.com/us/blog/threat-insight/bazaflix-bazaloader-fakes-movie-streaming-service.

[9] FBI Cyber Division. Silent Ransom Group Targeting Law Firms. 23 May 2025. https://www.ic3.gov/CSA/2025/250523.pdf.

[10] LOLRMM. https://lolrmm.io/.

[11] Malpedia. AsyncRAT. https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat.

[12] tajiknomi / BrowserCredExtractor_windows. https://github.com/tajiknomi/BrowserCredExtractor_windows/blob/main/Extract%20Master%20Keys/src/BrowserKeyExtract.cpp.

[13] Malpedia. UAC-0050. https://malpedia.caad.fkie.fraunhofer.de/actor/uac-0050.

[14] Miller, D. Are You Sure Your Browser is Up to Date? The Current Landscape of Fake Browser Updates. Proofpoint. 17 October 2023. https://www.proofpoint.com/us/blog/threat-insight/are-you-sure-your-browser-date-current-landscape-fake-browser-updates.