Remote Monitoring and Management (RMM) Tooling Increasingly an Attacker’s First Choice

proofpoint.com/us/blog/threat-insight/remote-monitoring-and-management-rmm-tooling-increasingly-attackers-first-choice

March 5, 2025

Share with your network!

March 07, 2025 Ole Villadsen, Selena Larson, and The Proofpoint Threat Research Team

Key findings

- More threat actors are using legitimate remote monitoring and management (RMM) tools as a first-stage payload in email campaigns.
- RMMs can be used for data collection, financial theft, lateral movement, and to install follow-on malware including ransomware.
- While threat actors have long used RMMs in campaigns and attack chains, their increased use as a first-stage payload in email data is notable.
- The increase in RMM tooling aligns with a decrease in prominent loaders and botnets typically used by initial access brokers.

Overview

More threat actors are using legitimate RMM tools (or in some cases, remote access software) in email campaigns as a first-stage payload for cyberattacks. RMM software is used legitimately in enterprises for information technology (IT) administrators to remotely manage fleets of computers. When abused, such software has the same capabilities as remote access trojans (RATs) and financially motivated threats are delivering RMM tools more often via email.

In 2024, Proofpoint researchers observed a notable increase in the use of RMM tools from cybercriminal threat actors in documented campaigns, including using payloads such as ScreenConnect, Fleetdeck, and Atera. A campaign is defined by Proofpoint as a timebound set of related threat activity analyzed by Proofpoint researchers. Notably, while NetSupport had historically been the most frequently observed RMM in Proofpoint campaign data, its use dropped off throughout 2024 and other RMMs became much more prominent. This trend is continuing in 2025.

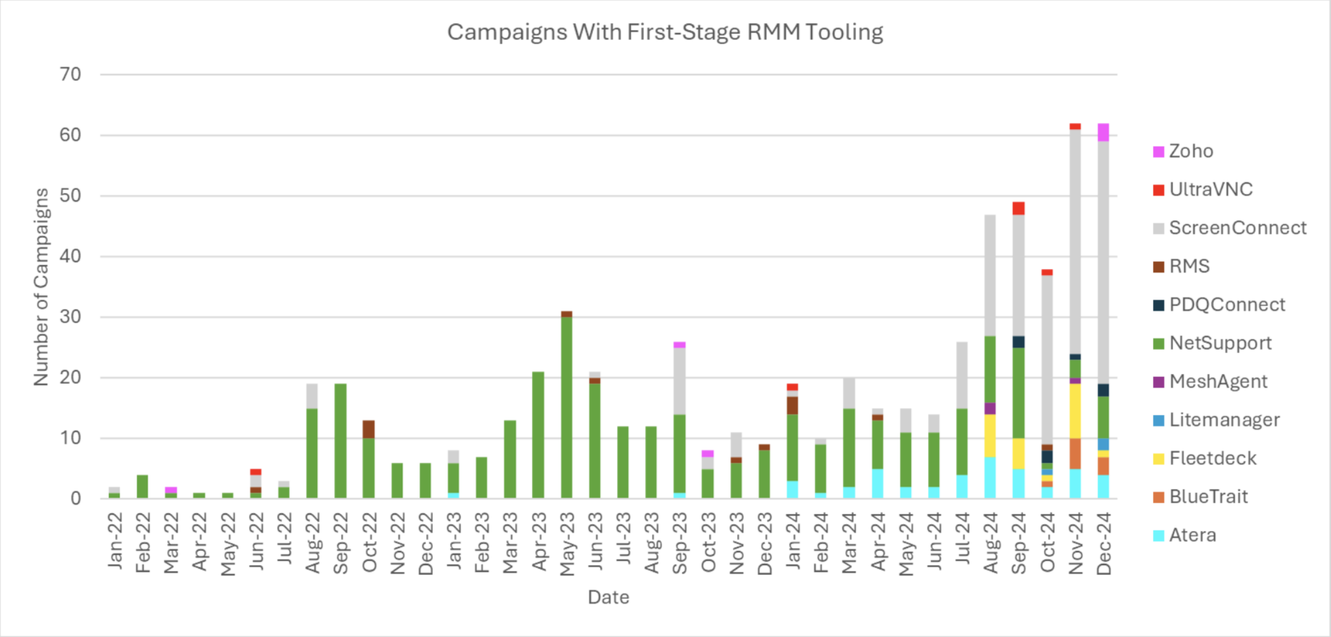
The increased use of RMM tooling also aligns with a decrease in prominent loader and botnet malware most often used by initial access brokers in the realm of ecrime.

RMMs and IABs

Typically in attacks like ransomware, RMMs are used as part of an overall attack chain, and observed as a follow-on payload or technique once initial access has been achieved. The infection could originate through a loader delivered via email, or some other method. The use of RMMs in malicious activity is common, and threat actors can abuse these tools in many ways including leveraging existing remote administration tools within an environment or installing new RMM software on a compromised host for persistence and lateral movement.

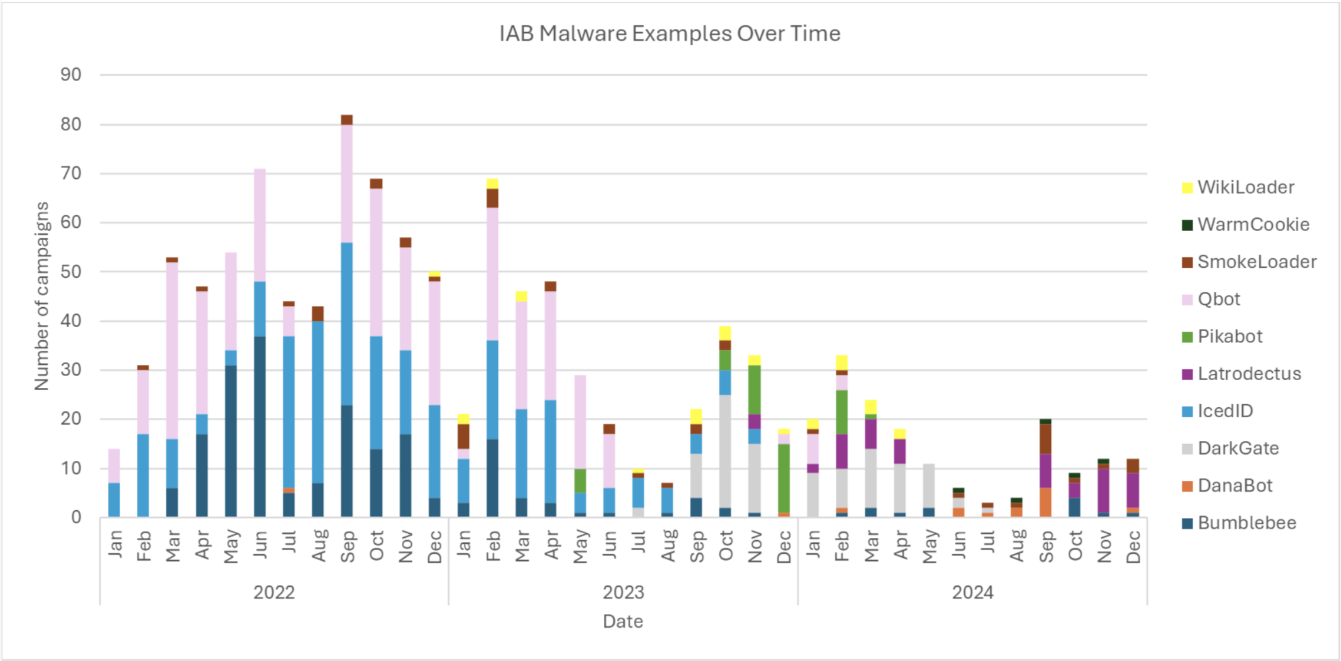
Threat actors conducting telephone-oriented attack delivery (TOAD) attacks frequently use RMM tools. In these attacks, a threat actor will send an email with a phone number included either in the body text or an attached PDF, typically using invoice lures. The recipient is instructed to call the phone number to dispute the invoice, but the phone number belongs to the threat actor who will ultimately direct the recipient to install an RMM or other malware once they get them on the phone. Payloads typically delivered by TOAD actors include AnyDesk, TeamViewer, Zoho, UltraViewer, NetSupport, and ScreenConnect.

The use of RMMs as a first-stage payload delivered directly via email was not as common as other malware delivery in Proofpoint campaign data prior to 2024, with most of such campaigns since 2022 delivering NetSupport. However, the presence of RMMs in campaign data began increasing in mid-2024, with ScreenConnect in particular appearing much more frequently.



Campaigns from January 2022 through December 2024 that include RMM tooling.

Interestingly, the increase of RMMs observed in Proofpoint data aligns with the decrease in observed loaders and botnets popular with initial access brokers (IABs) in email campaign data, which historically comprised a large part of the overall threat landscape. Proofpoint has observed multiple tracked IABs considerably decrease activity or disappear altogether from email campaign data since mid-2024, including TA577, TA571, and TA544. It is likely these actors are either retooling or using other initial access methods instead of email. For example, TA577 campaigns have previously been observed leading to Black Basta ransomware. Third-party reporting on recent Black Basta incidents indicate initial access began via social engineering attacks leveraging Microsoft Teams.



Campaigns associated with malware used by IAB threat actors in email threat data, 2022 - 2024.

The decrease in IAB email threat activity is most likely due to Operation Endgame, a global law enforcement effort that disrupted the infrastructure of IcedID, SystemBC, Pikabot, SmokeLoader, Bumblebee, and Trickbot. With limited access to these major malware families, IAB threat actors could not conduct their typical email-based attacks. Ransomware payments overall also declined in the second half of 2024, according to reporting from blockchain intelligence firm Chainalysis. Payments overall fell 35% in 2024.

Proofpoint does not attribute many of the of RMM campaigns to tracked threat actors, so the IAB actors tracked by our researchers have not necessarily pivoted to RMM delivery via email. However, it is interesting to note the drastic shift in the landscape throughout 2024, and the increase in new and different tooling following the disruption of major botnets and loaders.

While the RMM campaign volumes have increased, the message volumes range from just a handful of messages to thousands per campaign. But the overall message volume is still lower than historic IAB malspam activity.

Notably, according to information shared with Proofpoint by our colleagues at Red Canary and DFIR Report, who specialize in tracking and remediating post-exploitation activity, the most popular RMMs used as second-stage payloads are not the same as the ones most frequently observed as first-stage payloads in Proofpoint data. Based on analysis of Emerging Threats detections fired, according to data via OPNsense users running ETPRO Telemetry Edition, the most prominent RMM appearing in network activity is TeamViewer, followed by Atera and NetSupport appearing much less frequently in data. (This is based on detections firing, not confirmed malicious use.)

Campaign examples

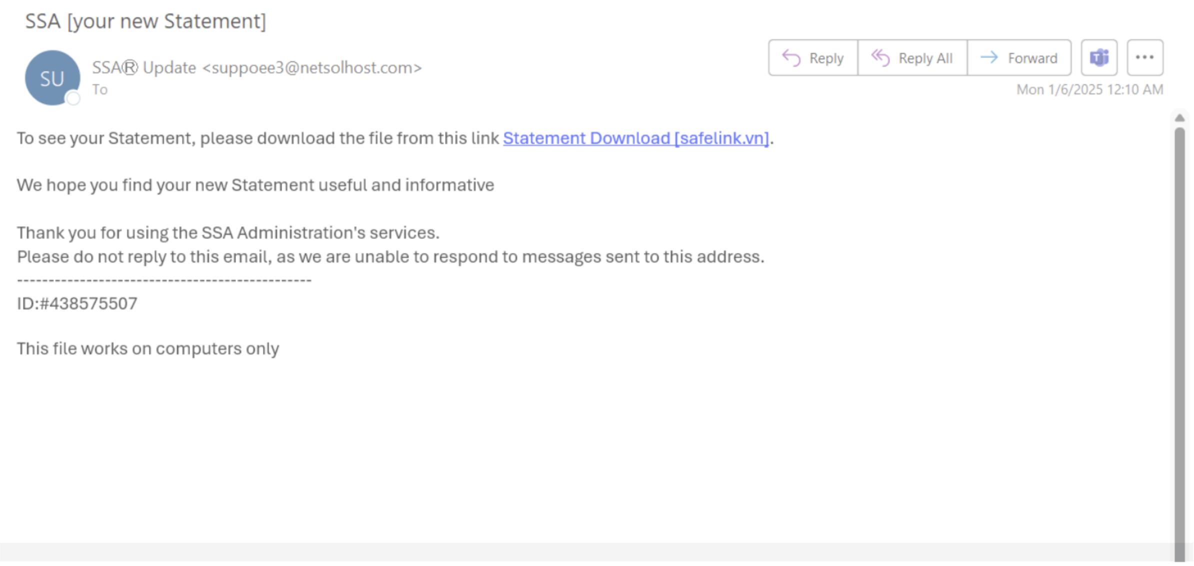
TA583

Proofpoint recently designated a new threat actor, TA583. TA583 is one of the most prominent threat activity sets distributing ScreenConnect. It’s currently a highly active threat actor that conducts multiple campaigns each day, most of which use this RMM. The size and scope of the campaigns vary, with some including tens of thousands of messages, while others may target only a few people in Proofpoint’s telemetry.

TA583 is a cybercriminal threat actor with the goal of obtaining remote access in target environments. Specific objectives once a system is compromised are outside of Proofpoint’s visibility, but may include account take over (ATO), credential theft, data exfiltration, and possibly brokering initial access for other threat actors. Proofpoint has tracked this actor since 2022 through email lures, targeting, malware used, and network infrastructure, but only designated a TA number in January 2025. Prior to mid-2024, this actor mostly deployed AsyncRAT and used ScreenConnect as a first stage payload less frequently. However, since mid-2024, the actor has primarily used ScreenConnect as an initial access payload. Proofpoint has also observed ScreenConnect on several occasions download and install AsyncRAT following an infection, suggesting that the RMM is used frequently as a loader for other malware.

Currently, most observed campaigns deliver ScreenConnect using URLs, although many also employ HTML or PDF attachments. These URLs frequently use email shortener services and publicly available services such as Dropbox and Bitbucket. This actor routinely uses lures related to the U.S. Social Security Administration. Other observed lures include the Canada Pension Plan, U.S. Internal Revenue Service, U.S. Postal Service (USPS), various telecommunications providers, and more.

For example, on 6 January 2025, Proofpoint identified a campaign impersonating the U.S. Social Security Administration. Messages contained URLs leading to an executable, which, if executed, installed ScreenConnect.



SSA [your new Statement]

SSA® Update <suppoee3@netsolhost.com>
To

Mon 1/6/2025 12:10 AM

To see your Statement, please download the file from this link Statement Download [safelink.vn].

We hope you find your new Statement useful and informative

Thank you for using the SSA Administration's services.
Please do not reply to this email, as we are unable to respond to messages sent to this address.

ID:#438575507

This file works on computers only

TA583 lure impersonating the U.S. Social Security Administration.

To deliver emails, Proofpoint has observed TA583 commonly use the following methods:

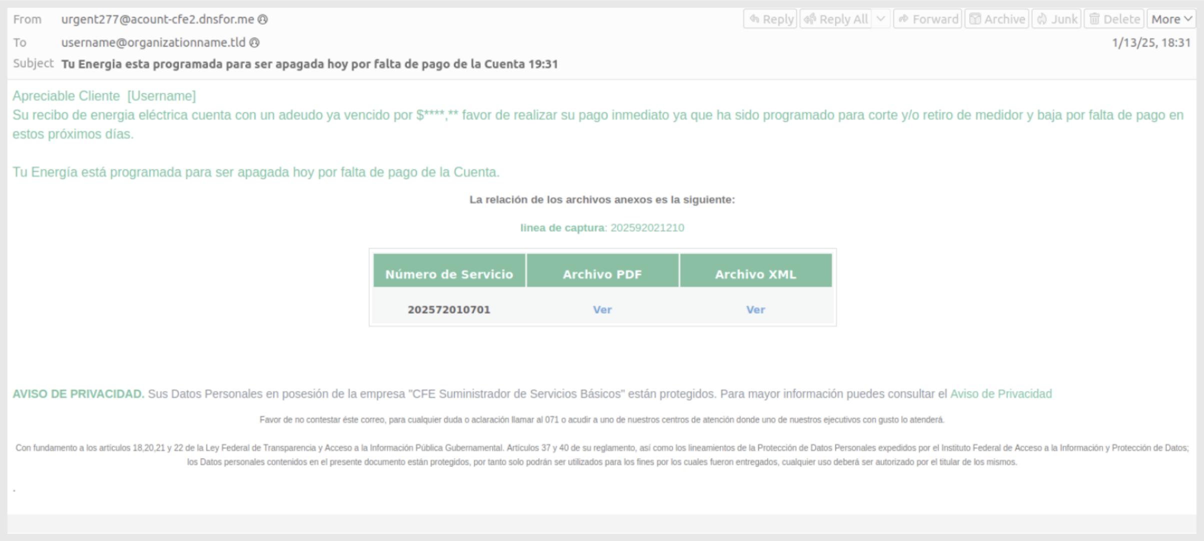
- Free consumer email accounts provided by telecommunications providers
- Email marketing and survey platforms (e.g. Sendgrid, Mailjet, and Qualtrics)
- Compromised email accounts

TA583 uses legitimate, signed ScreenConnect installers and uses both DDNS providers as well as actor-owned command and control (C2) servers.

TA2725

Other threat actors have adopted RMM tooling as a first stage payload, including TA2725. TA2725 is a threat actor Proofpoint tracked since March 2022 that is known for using Brazilian banking malware (including Mispadu, Astaroth, and historically Grandoreiro) and credential phishing to target organizations mainly in Brazil, Mexico, and Spain. TA2725 typically hosts their URL redirector on GoDaddy virtual hosting.

In January 2025, TA2725 began delivering ScreenConnect for the first time. The campaigns included energy bill lures with URLs leading to compressed executables that led to the installation of ScreenConnect. These campaigns exclusively targeted organizations in Mexico.



From urgent277@acount-cfe2.dnsfor.me
To username@organizationname.tld
Subject **Tu Energia esta programada para ser apagada hoy por falta de pago de la Cuenta 19:31**

1/13/25, 18:31

Apreciable Cliente [Username]
Su recibo de energia eléctrica cuenta con un adeudo ya vencido por $****,** favor de realizar su pago inmediato ya que ha sido programado para corte y/o retiro de medidor y baja por falta de pago en estos próximos días.

Tu Energía está programada para ser apagada hoy por falta de pago de la Cuenta.

La relación de los archivos anexos es la siguiente:

linea de captura: 202592021210

Número de Servicio	Archivo PDF	Archivo XML
202572010701	Ver	Ver

AVISO DE PRIVACIDAD. Sus Datos Personales en posesión de la empresa "CFE Suministrador de Servicios Básicos" están protegidos. Para mayor información puedes consultar el Aviso de Privacidad

Favor de no contestar éste correo, para cualquier duda o aclaración llamar al 071 o acudir a uno de nuestros centros de atención donde uno de nuestros ejecutivos con gusto lo atenderá.

Con fundamento a los artículos 18,20,21 y 22 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Artículos 37 y 40 de su reglamento, así como los lineamientos de la Protección de Datos Personales expedidos por el Instituto Federal de Acceso a la Información y Protección de Datos; los Datos personales contenidos en el presente documento están protegidos, por tanto solo podrán ser utilizados para los fines por los cuales fueron entregados, cualquier uso deberá ser autorizado por el titular de los mismos.

.

Spanish language TA2725 campaign observed on 14 January 2025 delivering ScreenConnect.

It is likely that more cybercriminal threat actors will adopt RMM tooling as a first stage payload given the expansion and efficacy of other groups using such payloads.

ZPHP and UAC-0050

While NetSupport is less commonly observed in Proofpoint campaign data at this time, there are still a handful of threat actors that distribute it as a first-stage payload via email.

For example, Proofpoint first identified a cluster of fake update campaigns leading to NetSupport RAT in June 2023. Proofpoint calls this activity ZPHP, and its activity is ongoing with weekly campaigns. The ZPHP inject is a simple script object that is added into a compromised website's HTML code. The payload is downloaded via a base64 encoded zip file. The zipped browser update payload usually contains a JavaScript file that will load a malicious NetSupport RAT payload onto the host. Proofpoint has also seen the .zip contain an executable that loaded Lumma Stealer.

Notably, the current NetSupport configuration includes the following:

```
Licensee: XMLCTL
SerialNumber: NSM303008
```

Researchers first observed ZPHP use this license in June 2024, and it has been used in ZPHP campaigns ever since.

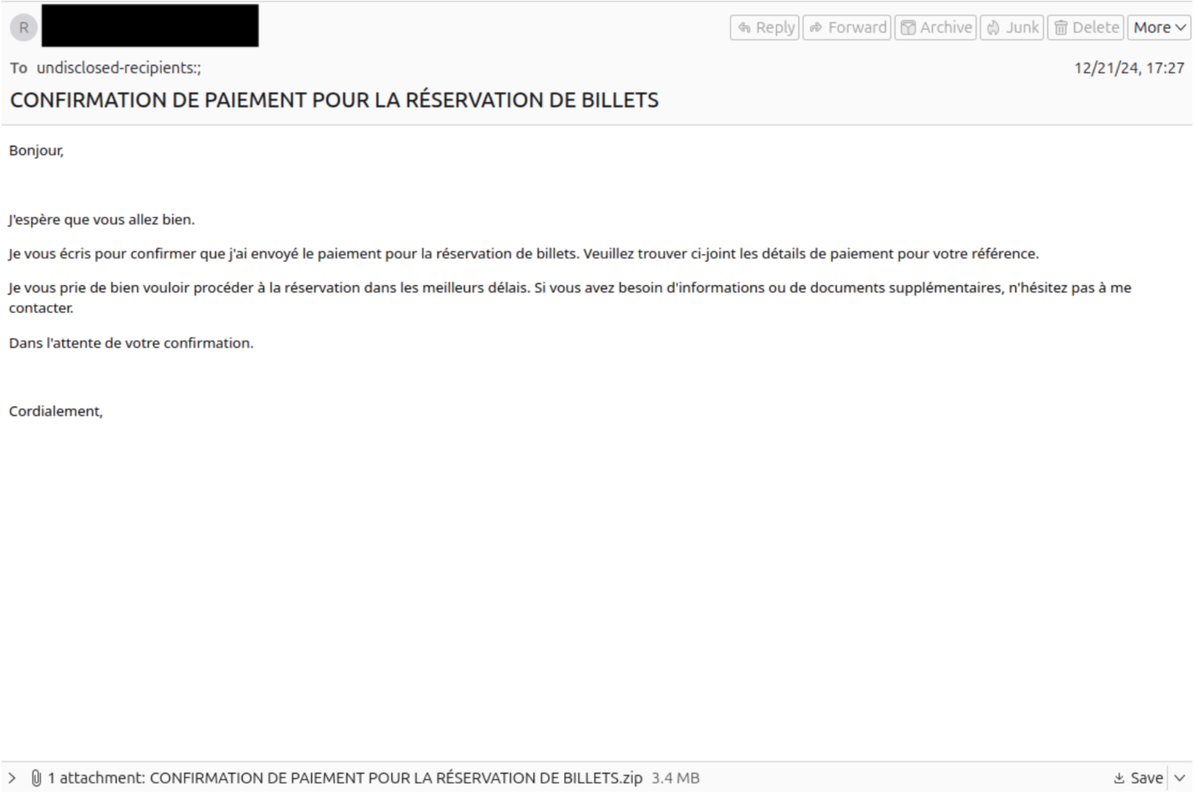
Notably, that license overlaps with NetSupport payloads recently delivered by UAC-0050, a threat actor that typically targets organizations in Ukraine with remote access trojans (RATs). On 14 January 2025, Proofpoint researchers observed this actor deliver zipped PDFs with URLs ultimately leading to the installation of NetSupport with the license “XMLCTL”. This was the first time Proofpoint observed UAC-0050 deliver NetSupport, as it has historically used other malware including Remcos and Lumma Stealer, but it has previously used RMMs including Litemanager and Remote Manipulator System (RMS). Researchers observed three subsequent UAC-0050 NetSupport campaigns with the same license in January.

In addition to the license, UAC-0050 also uses a similar delivery mechanism as ZPHP, with URLs leading to JavaScript files which will download a ZIP file containing the NetSupport payload. Additionally, the JavaScript code used by both actors is similar; while the variable and function naming conventions are slightly different, the script itself is functionally identical.

The overlapping NetSupport configuration and code similarities 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 and delivery method.

French targeted RMM

Bluetrait is an RMM not frequently observed in Proofpoint data, however at least one threat activity cluster has used Bluetrait regularly since October 2024. Campaigns are typically low volume, ranging from a handful to less than 500 messages per campaign. Messages are typically written in French or English and include payment themed lures. For example, Proofpoint observed a campaign on 21 December 2024 using ticket reservation payment themes.



[redacted]

To undisclosed-recipients:; 12/21/24, 17:27

CONFIRMATION DE PAIEMENT POUR LA RÉSERVATION DE BILLETS

Bonjour,

J'espère que vous allez bien.

Je vous écris pour confirmer que j'ai envoyé le paiement pour la réservation de billets. Veuillez trouver ci-joint les détails de paiement pour votre référence.

Je vous prie de bien vouloir procéder à la réservation dans les meilleurs délais. Si vous avez besoin d'informations ou de documents supplémentaires, n'hésitez pas à me contacter.

Dans l'attente de votre confirmation.

Cordialement,

1 attachment: CONFIRMATION DE PAIEMENT POUR LA RÉSERVATION DE BILLETS.zip 3.4 MB

French language email distributing Bluetrait.

In this campaign, messages contained compressed MSI attachments which, if executed, installed Bluetrait. This cluster of activity primarily uses PDFs with URLs leading to a compressed MSI attachment and, to a lesser extent, MSI attachments directly in the email. The MSI files lead to the installation of Bluetrait. Notably, this threat cluster also delivers the Fleetdeck RMM using similar lures and methods.

Best practices

As threat actors are increasingly using legitimate RMM tools in malware campaigns, Proofpoint recommends the following:

- Restrict the download and installation of any RMM tooling that is not approved and confirmed by an organization’s information technology administrators.
- Have network detections in place – including using the Emerging Threats ruleset – and use endpoint protection. This can alert on any network activity to RMM servers.
- Train users to identify the activity and report suspicious activity to their security teams. This training can easily be integrated into an existing user training program.

Conclusion

Proofpoint anticipates the use of RMM tooling as a first-stage payload will increase. It’s fairly easy for threat actors to create and distribute attacker-owned remote monitoring tools, and because they are often used as legitimate pieces of software, end users might be less suspicious of installing RMMs than other remote access trojans. Additionally, such tooling may evade anti-virus or network detection because the installers are often signed, legitimate payloads distributed maliciously.

Proofpoint would like to thank our colleagues at ConnectWise ScreenConnect, Red Canary, and DFIR Report for collaborating on information sharing related to this activity.

Example ET signatures

2837962 – ScreenConnect - Establish Connection Attempt

2836266 – TeamViewer HTTP Checkin

2857201 – Atera DMM Related Domain in DNS Lookup

2056777 – RMM Software Domain in DNS Lookup (bluetrait .io)

2054938 – PDQ Remote Management Agent Checkin

2833909 – UltraVnc Session Outbound

Example IOCs

Indicator
hxxps://region-businesss-esignals.s3.us-east-1.amazonaws[.]com/region-businesss-esignals-46980.html
hxxps://ssastatementshelpcenter[.]de/top/
hxxps://retireafter5m[.]co/Bin/Recently_S_S_A_eStatementForum_Viewr5406991387785667481_Pdf.Client.exe?e=Access&y=Guest&s=1fa7623
retireafter5m[.]co
hxxps://safelink[.]vn/OsDXr
hxxps://safelink[.]vn/GESLx
hxxp://www[.]farrarscieng[.]com/re[.]php
hxxps://3650ffice[.]anticlouds[.]su/Fraud_Alert_black/
hxxps://online[.]invoicesing[.]es/Bin/Statement[.]ClientSetup[.]exe?e=Access&y=Guest&c=Black_Cat&c=&c=&c=&c=&c=&c=&c=\
hxxps://online[.]invoicesing[.]es/Bin/Attachment[.]Client[.]exe?h=instance-w08c5r-relay[.]screenconnect[.]com&p=443&k=BgIAAACkAABSU0ExAAgAAAEAAQBtb%2FXciCJO5hHyAR3NG5qwkHgKE4K5jxeGBs35NIncjh1l6g%2B 6914-4689-8deb-67789c4f3a34&i=&e=Support&y=Guest&r=
invoice007[.]zapto[.]org
b8fd2b4601b09aacd760fbede937232349bf90c23b35564ae538ed13313c7bd0
instance-udm3tv-relay[.]screenconnect[.]com
109[.]71[.]247[.]168

hxxp://45[.]155[.]249[.]215/xxx.zip
97b35a7673ae59585ad39d99e20d9028ac26bbccb50f2302516520f544fe637e
185[.]157[.]213[.]71:443
4c4e15513337db5e0833133f587e0ed131d4ebb65bb9a3d6b62a868407aae070
hxxps://kalika[.]bluetrait[.]io/api/

Previous Blog Post

Subscribe to the Proofpoint Blog