ProxyShell, QBot, and Conti ransomware combined in a series of cyber attacks - Truesec

By siteadmin

Published: 2021-11-15 · Archived: 2026-04-05 19:04:08 UTC

A Truesec investigation

We are investigating a series of cyber attacks that result in encryption with the Conti ransomware. This post describes some of the indicators that can be used to detect these attacks.

Attack Overview

First, unpatched Exchange servers are exploited using ProxyShell. Compromised servers are then used to spread phishing emails delivering Datoploader (aka Squirrelwaffle) and the QBot trojan. The threat actor here is likely an access broker specializing in selling access to other cybercriminals.

Attack Overview – Stage 1 – ProxyShell Exploit

Access to infected computers is then handed over to a different group, which then proceeds to launch Cobalt Strike beacons managed from a different infrastructure. This threat actor is likely an affiliate of the Conti gang (or “pentester” as they call it) whose job it is to escalate in the internal network.

Attack Overview – Stage 2 – Access Handover

In the final stage the Conti gang takes over, deletes backups, and ultimately deploys the Conti ransomware.

Attack Overview – Stage 3 – Conti Ransomware

ProxyShell and Mass Phishing

ProxyShell is nothing new, but there are still systems that have not been patched in the past few months.

We have identified multiple cases of Exchange servers compromised with ProxyShell (chaining CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) in September and October.

Starting from early November, the compromised Exchange servers have been used to launch phishing attacks.

Although the content of the phishing emails looks very suspicious, this attack hijacks existing email threads and also adjusts the language based on the language appearing in the email thread. This makes it more likely for a victim to follow the instructions.

An example in English is shown below.

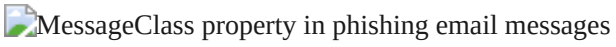

Example of a phishing email in English

The following example is in Swedish, as the hijacked conversation was in Swedish.


Example of a phishing email in Swedish

The links in the emails vary a lot and cannot be used to consistently identify phishing emails as part of this campaign.

However, we have identified that the following MessageClass property seems to be consistently used in all phishing emails.


MessageClass property in phishing email messages

We can therefore search for **MessageClass:IPM.Blabla** in the following logs on the Exchange server to find likely phishing emails being sent.


Exchange Message Tracking logs

Datoploader and QBot Infections

The links in the email direct the victims to websites serving malicious .ZIP files.

The .ZIP files contain macro-enabled Excel (.XLS) files, as shown below.


Macro enabled Excel file

As in any other classic phishing attack, when opened, the XLS files present an image to the user, with instructions to enable macro execution.

The XLS macros are obfuscated by building each of the actual command characters from content of various cells in the document.


Obfuscated macro

When executed, the macros create the directory “C:Datop”, download three files to this directory, and run them using regsvr32.exe.


Deobfuscated macro


Execution using regsvr32.exe

Persistence

So far we have identified two ways that the malware made itself persistent. An autorun registry key launching regsvr32.exe to execute a DLL, and a scheduled task launching PowerShell which in turn starts regsvr32.exe in the same way.


Persistence – Registry Autorun Key


Persistence – Scheduled Task

Cobalt Strike

Within minutes (sometimes hours) from the Datoploader / QBot infection, the threat actor launched Cobalt Strike. This seems to be a plugin built into Qbot.


QBot debug messages

Enumeration and Lateral Movement

Shortly after the Cobalt Strike execution, the threat actor starts manually interacting with the compromised network, first by enumerating and escalating within Active Directory, and later by deploying Cobalt Strike on additionally compromised servers. Escalation to domain admin is quickly achieved.

As an additional backdoor into some of the compromised systems, the threat actor creates a local account named ‘Crackenn’.

The threat actor uses the following command to enumerate workstations in the domain:

```
$so = New-Object System.DirectoryServices.DirectorySearcher; $so.filter = "(&(samAccountType=8053063
```

Additionally, the following command is used to retrieve all computers within the domain.

```
import-module activedirectory; Get-ADComputer -Filter * -Properties * | Sort OperatingSystem | Selec
```

Once high privileges are obtained, the threat actor uses both Cobalt Strike beacons and Remote Desktop (RDP) connections to identify sensitive business data to exfiltrate.

The last stage of the attack is the deployment of the Conti ransomware.

What To Do if You Received the Phishing Emails

If users in your organization have received emails like the ones described in this article, ensure that a thorough analysis is performed on the accounts and computers of the individuals receiving the emails.

At the very least, check the indicators of compromise below. Consider, however, that files and domains used in these campaigns constantly change. A consistent indicator so far has been the presence of the directory “C:Datop” on computers infected with Datoploader from the phishing attack.

Keep in mind that if you find indicators of compromise, it is not sufficient to clean/reinstall the system. It is likely that the compromised system was used to spread to additional computers in the network. Perform a thorough investigation or ask for help if you don’t have in-house incident response capabilities.

Indicators of Compromise

MessageClass in phishing email messages

- MessageClass:IPM.Blabla

Directory for Datoploader

- C:Datop

ZIP files delivering Datoploader

- bda187d62d5e48c3dee06ee11397e2456457d0b3c766dc6b453abb32f1d49196 (minimaaliquid-2738715.zip)
- b2b4f9f38cee7243679afce0348ac7217abb73285fe69b15950c114964c9f131 (omnisvelit-2738715 (1).zip)
- a1b79c1dff2c7e1175611f6d1d45f05a2cee74e3d2ee45b913f73e30f8a9a66e (omnisvelit-2738715.zip)
- cb59bf0e135fc620aeddd8334b537150b7057f06375fe2f86ca91e722f7006f3 (uteligendi-2387259 (1).zip)
- d4dd05bd12e85fca9bfd823e093b16ec8eac9fb65db9e61015788f7fe688f920 (uteligendi-2387259.zip)
- 6a20d87b61401bc7985aed6d951efee66388a9d522e0e15aed6f5d846953dbf9 (content-1824738050.xls)
- 95847fc69ddc4736d817430ffb49f8c41eb8bc5a03fa40e7081748f28f95f1c2 (content-1848283165.xls)
- b298f3497cf739a73350e8007220083f9e37a13e12390c5624b0075ea880e9db (content-1845165288.xls)
- 236338b58b929694a29321802754e6e5a37fffd88798b7ef5d768bc5adcde93b (content-1861748987.xls)
- 705a292bb67b7a344d32937ca8cf86a1a10f9b25689fdf2df1401ffb4bdfd40d (content-1860852480.xls)

URLs in macros

- hxxps[:]//decinformatica[.]com/AsqpQT6a2fl/t.html
- hxxps[:]//novamiron[.]com.ar/SpV029NncEoH/t.html
- hxxps[:]//mooca.imprimeja[.]com.br/uqJeyCxO9/t.html
- hxxps[:]//taketuitions.com/dTEOdMByori/j.html
- hxxps[:]//constructorachg.cl/eFSLb6eV/j.html
- hxxps[:]//oel.tg/MSOFjh0EXRR8/j.html

Account created by threat actor

- Crackenn

Cobalt Strike servers

- 51.89.227.111
- 89.238.185.9
- 185.253.96.124
- 45.141.84.223

Files used during escalation

- ccccOUT.csv (Output of AD enum)
- adfind.ps1 (Script to import activedirectory module and run Get-ADComputer with -Properties *)
- 84CE00208FE4E2B46B26E4C9E058DF5341E90DA1FB1C0DBCBF207DB87F3DD991 (adfind.ps1)
- hv22.ps1 (Powershell function that scans the environment for forests and returns a list of Hyper-V Hosts within all domains of those forests)
- B37DFF29C62659E90034740F2BCA514F09C8EC3E507B8E0807933EE427875ACA (hv22.ps1)
- ppp.ps1 (Script to perform scanning activities)
- pc.csv (Referenced in ppp.ps1)
- a1.txt (Referenced in ppp.ps1)
