Threat Group Assessment: Turla (aka Pensive Ursa)

Unit 42 ⋮⋮ 9/15/2023

By Unit 42

September 15, 2023 at 6:00 AM

Category: Threat Advisory/Analysis, Threat Briefs and Assessments

This post is also available in: 日本語 (Japanese)

Executive Summary

Turla (aka Pensive Ursa, Uroburos, Snake) is a Russian-based threat group operating since at least 2004, which is linked to the Russian Federal Security Service (FSB). In this article, we will cover the top 10 most recently active types of malware in Pensive Ursa's arsenal: Capibar, Kazuar, Snake, Kopiluwak, QUIETCANARY/Tunnus, Crutch, ComRAT, Carbon, HyperStack and TinyTurla.

Pensive Ursa was chosen to be the main focus for the 2023 MITRE ATT&CK evaluation. MITRE has described Turla as being "known for their targeted intrusions and innovative stealth." The results of this evaluation, including Palo Alto Networks scoring, will be published in late September 2023.

In addition to describing each type of malware's functionality and history, we will present their execution through the lens of the Palo Alto Networks Cortex XDR product. We will show how Cortex protects against such malware, and the MITRE ATT&CK mapping of such threats as shown in the Cortex XDR platform.

Palo Alto Networks customers receive protections from Pensive Ursa's arsenal and the techniques discussed in this blog through Cortex XDR, which provides a multilayer defense that includes behavioral threat protection and exploit protection.

The Advanced WildFire cloud-delivered malware analysis service accurately identifies samples related to Pensive Ursa as malicious. Cloud-Delivered Security Services, including Advanced URL Filtering and DNS Security, identify domains associated with this group as malicious.

Related Unit 42 Topics	**APT**, Malware
Pensive Ursa	Alternative names: Turla, Snake, Uroburos, Venomous Bear, Waterbug, Iron Hunter

Malware discussed Capibar, Kazuar, Snake, QUIETCANARY, Kopiluwak, Crutch, ComRAT, Carbon, HyperStack, TinyTurla

Table of Contents

Pensive Ursa (aka Turla) Overview

Over the years, Pensive Ursa has become known as an advanced and elusive adversary. The group has demonstrated a high level of technical expertise, while orchestrating targeted and stealthy attacks.

As described by MITRE, Pensive Ursa targeted victims in over 45 countries as well as a wide range of sectors, including government entities, embassies, and military organizations, as well as education, research and pharmaceutical companies. In addition, this threat group had an active part in the Russian-Ukraine conflict that started in February 2022. According to the Ukraine CERT, Pensive Ursa leveraged espionage attacks against Ukrainian targets, specifically against their defense sector.

While Pensive Ursa mainly used their espionage arsenal to target Windows machines, the group also has tools that can attack macOS and Linux machines.

MITRE ATT&CK Evaluation

For the 2023 MITRE ATT&CK evaluation, Pensive Ursa was chosen to be the main focus. According to MITRE, this threat group is particularly relevant as their actions have global impact.

Below are the top 10 most recently active types of malware in the team's arsenal. For each type of malware, we provided a short description and analysis, as well as how Cortex XDR detects and prevents the threat.

Recent Pensive Ursa Arsenal Technical Analysis

Malware: Capibar

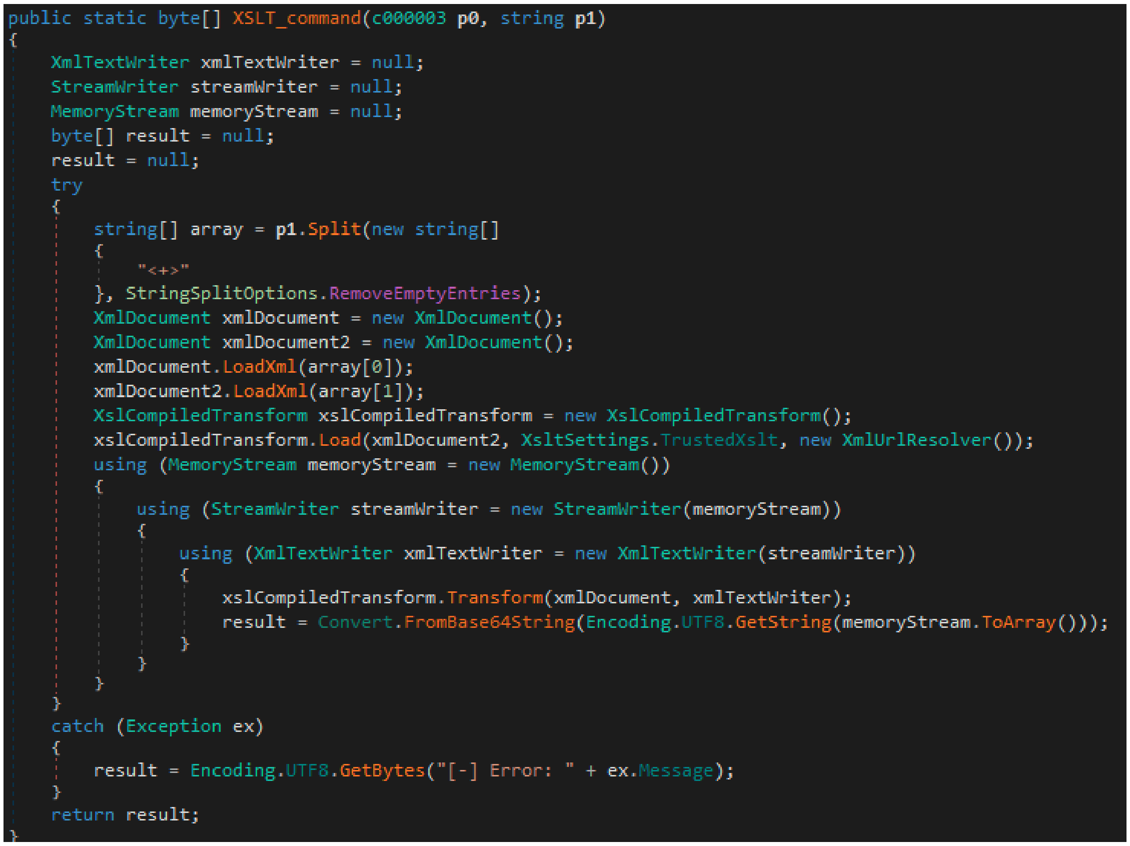
Aliases: DeliveryCheck, GAMEDAY

Malware Type: Backdoor

First Seen: 2022

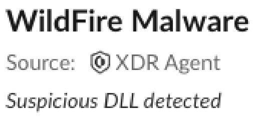
Description: Capibar (aka DeliveryCheck, GAMEDAY) is a Pensive Ursa backdoor that was first observed in 2022, and used for the purpose of espionage against defense forces in Ukraine. They distributed it via email as documents with malicious macros.

Capibar persists via a scheduled task that downloads and launches the payload in memory. The threat group installed Capibar on compromised MS Exchange servers as a Managed Object Format (MOF) file, granting the attacker full control of the server. Figure 1a below shows a snippet of the code responsible for loading XML received from its command and control (C2), and Figure 1b shows the alert triggered.



```
public static byte[] XSLT_command(c000003 p0, string p1)
{
    XmlTextWriter xmlTextWriter = null;
    StreamWriter streamWriter = null;
    MemoryStream memoryStream = null;
    byte[] result = null;
    result = null;
    try
    {
        string[] array = p1.Split(new string[]
        {
            "<+>"
        }, StringSplitOptions.RemoveEmptyEntries);
        XmlDocument xmlDocument = new XmlDocument();
        XmlDocument xmlDocument2 = new XmlDocument();
        xmlDocument.LoadXml(array[0]);
        xmlDocument2.LoadXml(array[1]);
        XslCompiledTransform xslCompiledTransform = new XslCompiledTransform();
        xslCompiledTransform.Load(xmlDocument2, XsltSettings.TrustedXslt, new XmlUrlResolver());
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (StreamWriter streamWriter = new StreamWriter(memoryStream))
            {
                using (XmlTextWriter xmlTextWriter = new XmlTextWriter(streamWriter))
                {
                    xslCompiledTransform.Transform(xmlDocument, xmlTextWriter);
                    result = Convert.FromBase64String(Encoding.UTF8.GetString(memoryStream.ToArray()));
                }
            }
        }
    }
    catch (Exception ex)
    {
        result = Encoding.UTF8.GetBytes("[-] Error: " + ex.Message);
    }
    return result;
}
```

Figure 1a. Capibar code snippet loading XML received from its C2.



WildFire Malware

Source: XDR Agent

Suspicious DLL detected

Figure 1b. The alert triggered in Cortex XDR.

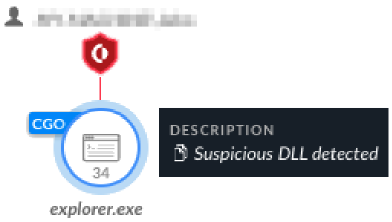
Malware: Kazuar

Malware Type: Backdoor

First Seen: 2017

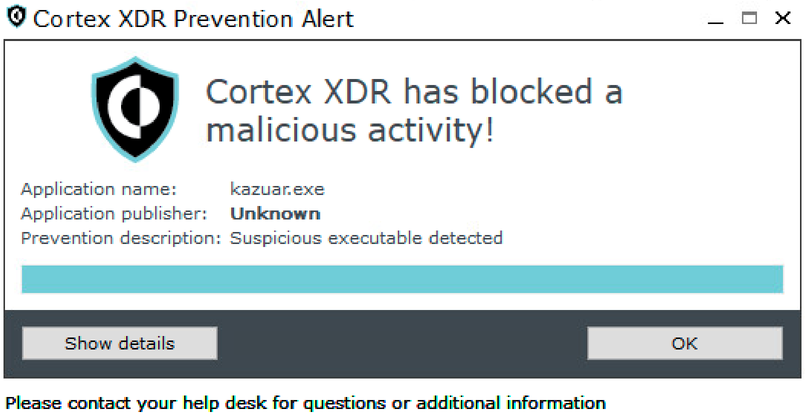
Description: Kazuar is a .NET backdoor that was discovered in 2017. Kazuar provides full access to the compromised systems targeted by its operator. Kazuar comes with a powerful command set that includes the ability to remotely load additional plugins to enhance the backdoor's capabilities.

In 2021, researchers found interesting code overlaps and similarities between Kazuar and the notorious SUNBURST backdoor that a Russian threat group used in the SolarWinds Operation. In July 2023, the Ukrainian CERT uncovered an espionage operation where Pensive Ursa used Kazuar as one of the main backdoors. Figure 2 shows Cortex XDR preventing a Kazuar DLL from being injected into the explorer.exe process, and Figure 3 shows an alert being triggered for Kazuar prevention.



DESCRIPTION
Suspicious DLL detected

Figure 2. Kazuar injected into explorer.exe and prevented by Cortex XDR.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: kazuar.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 3. Kazuar execution prevention alert by Cortex XDR.

Malware: Snake

Malware Type: Modular backdoor

First Seen: 2003

Description: The infamous Snake malware is the most complex tool in Pensive Ursa's tool set, as described by CISA in May 2023. The primary purpose of this tool is to achieve persistence for considerable periods of time and exfiltrate data from dedicated targets. It was in active development for 20 years, since 2003.

Snake was detected operating in more than 50 countries worldwide. The United States Department of Justice published a statement in which they announced Operation MEDUSA, where they disrupted the Snake malware activity and peer to peer (P2P) network. They did so by using a tool developed by the FBI dubbed PERSEUS, which they used as a kill switch for the Snake malware.

Based on previous analysis, the Snake malware implemented a maintainable code design, which showed that its authors had a high level of software development capability.

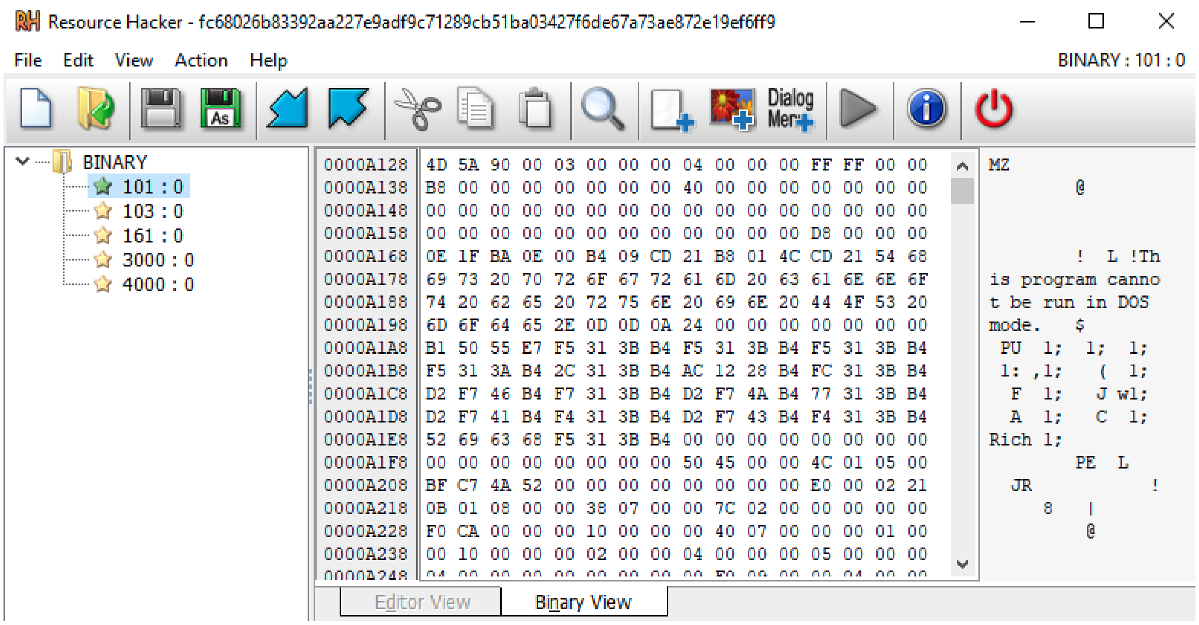
Snake implements features such as the following:

- A custom implementation of communication protocols over HTTP and TCP
- A kernel module for stealth
- Key logger functionality

More recent variants of Snake include an infection chain similar to the one depicted below.

Example of Snake Malware Delivery

Upon execution, Snake loads and executes Pensive Ursa's PNG Dropper malware from its resources and creates a hard-coded mutex {E9B1E207-B513-4cfc-86BE-6D6004E5CB9C, as shown in Figure 4.



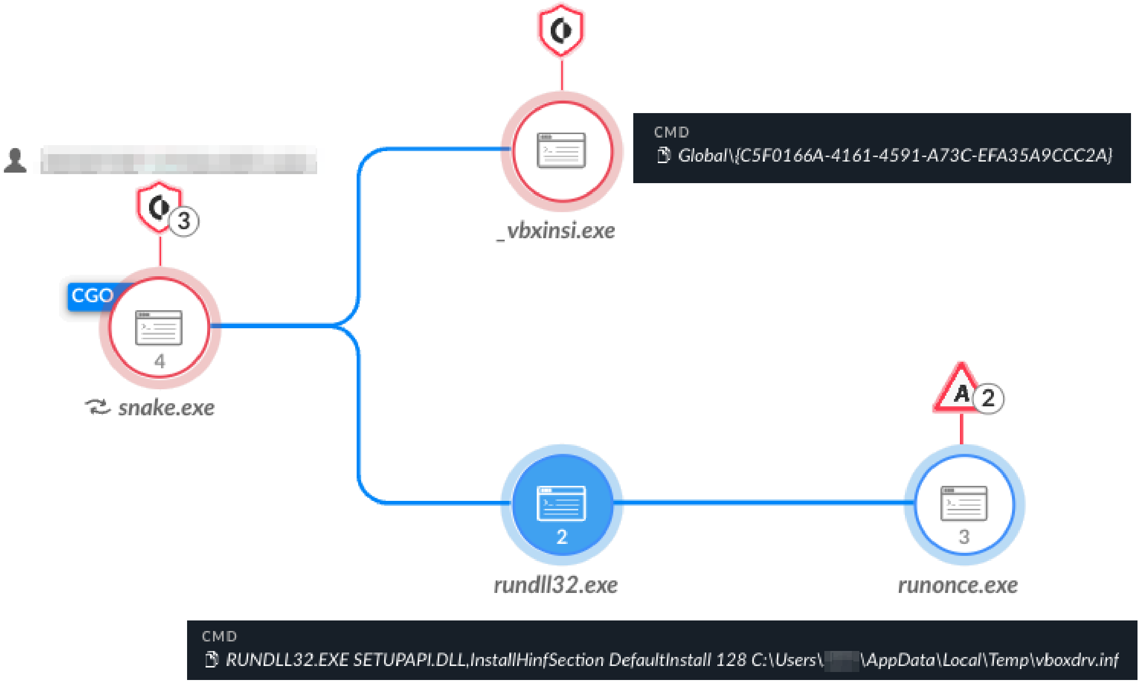
Resource Hacker - fc68026b83392aa227e9adf9c71289cb51ba03427f6de67a73ae872e19ef6ff9

```
0000A128  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ
0000A138  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00           @
0000A148  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000A158  00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00
0000A168  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68           !  L !Th
0000A178  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
0000A188  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
0000A198  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode.   $
0000A1A8  B1 50 55 E7 F5 31 3B B4 F5 31 3B B4 F5 31 3B B4    PU  l;  l;  l;
0000A1B8  F5 31 3A B4 2C 31 3B B4 AC 12 28 B4 FC 31 3B B4    l: ,l;   (  l;
0000A1C8  D2 F7 46 B4 F7 31 3B B4 D2 F7 4A B4 77 31 3B B4     F  l;   J wl;
0000A1D8  D2 F7 41 B4 F4 31 3B B4 D2 F7 43 B4 F4 31 3B B4     A  l;   C  l;
0000A1E8  52 69 63 68 F5 31 3B B4 00 00 00 00 00 00 00 00   Rich l;
0000A1F8  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00           PE  L
0000A208  BF C7 4A 52 00 00 00 00 00 00 00 00 E0 00 02 21     JR          !
0000A218  0B 01 08 00 00 38 07 00 00 7C 02 00 00 00 00 00        8   |
0000A228  F0 CA 00 00 00 10 00 00 00 40 07 00 00 00 01 00            @
0000A238  00 10 00 00 00 02 00 00 04 00 00 00 05 00 00 00
```

Figure 4. Snake loader’s resources.

The PNG dropper then decodes and loads a vulnerable VM driver that is used for privilege escalation in order to write the main Snake payload to disk, and register it as a service.

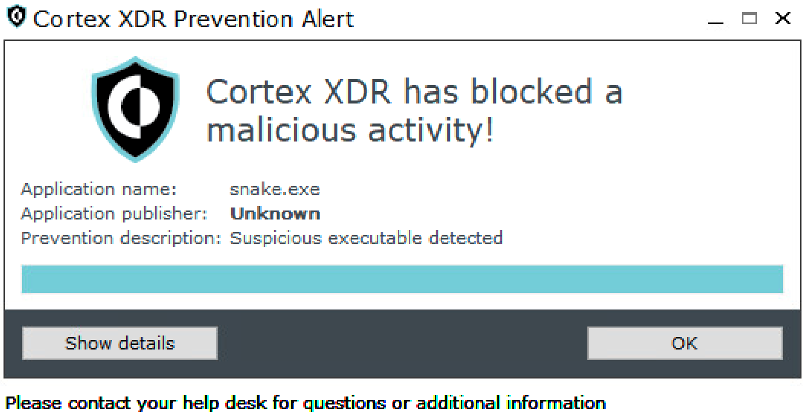
The Snake loader variant shown in Figure 5 detects the multiple stages in the infection chain that lead to the deployment, service registration and execution of the main Snake payload. Figure 6 shows the execution prevention alert pop-up in Cortex XDR.



CMD
Global\{C5F0166A-4161-4591-A73C-EFA35A9CCC2A}

CMD
RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultInstall 128 C:\Users\[redacted]\AppData\Local\Temp\vboxdrv.inf

Figure 5. Snake execution detection shown in Cortex XDR in detect mode.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: snake.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 6. Snake execution prevention alert shown in Cortex XDR.

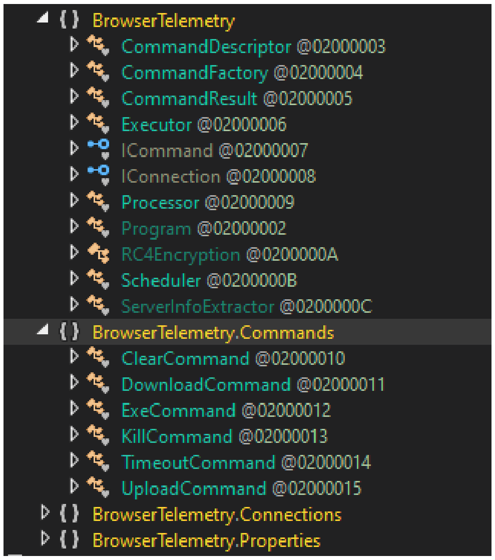
Malware: QUIETCANARY

Aliases: Tunnus

Malware Type: Backdoor

First Seen: 2017

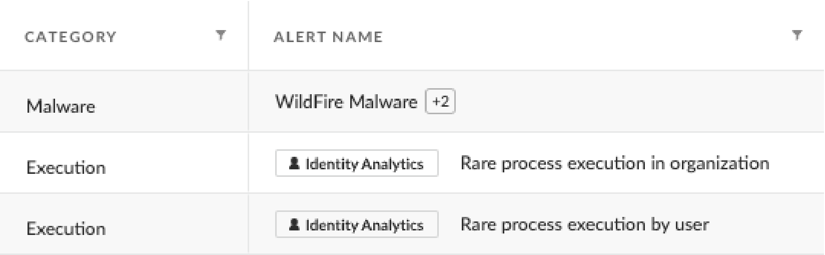
Description: Pensive Ursa has been observed using QUIETCANARY since 2019, and the Tomiris group has used this backdoor even earlier. Pensive Ursa deployed QUIETCANARY against targets in Ukraine in September 2022, together with the Kopiluwak malware. QUIETCANARY is a lightweight backdoor written in .NET, which is capable of executing various commands received from its C2 server, including downloading additional payloads and executing arbitrary commands. It also implements RC4 encryption to protect its C2 communication. Figure 7 shows QUIETCANARY's different classes that reveal its backdoor capabilities.



```
◢ { } BrowserTelemetry
    ▷ CommandDescriptor @02000003
    ▷ CommandFactory @02000004
    ▷ CommandResult @02000005
    ▷ Executor @02000006
    ▷ ICommand @02000007
    ▷ IConnection @02000008
    ▷ Processor @02000009
    ▷ Program @02000002
    ▷ RC4Encryption @0200000A
    ▷ Scheduler @0200000B
    ▷ ServerInfoExtractor @0200000C
◢ { } BrowserTelemetry.Commands
    ▷ ClearCommand @02000010
    ▷ DownloadCommand @02000011
    ▷ ExeCommand @02000012
    ▷ KillCommand @02000013
    ▷ TimeoutCommand @02000014
    ▷ UploadCommand @02000015
▷ { } BrowserTelemetry.Connections
▷ { } BrowserTelemetry.Properties
```

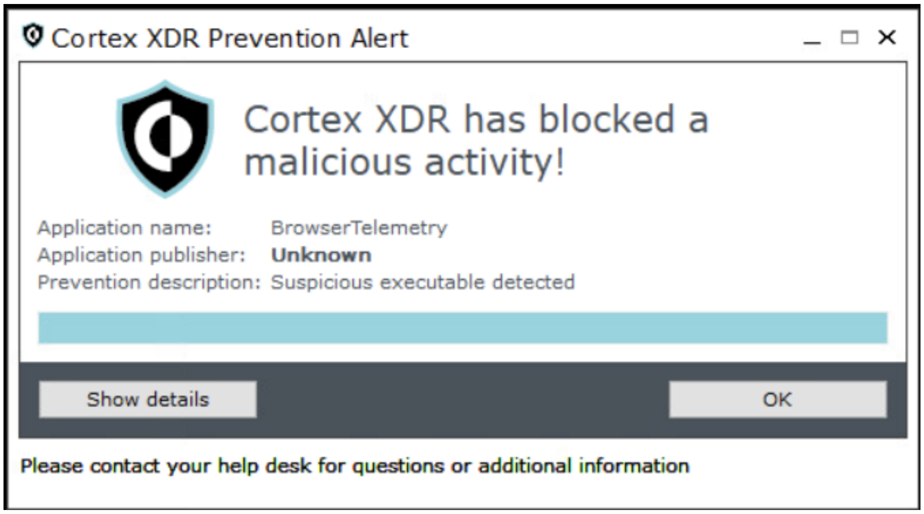
Figure 7. Code snippet of the different classes in QUIETCANARY's code.

Figure 8 shows the Cortex XDR multilayered protection-based alerts that QUIETCANARY triggered. Figure 9 shows the execution prevention alert.



CATEGORY	ALERT NAME
Malware	WildFire Malware +2
Execution	Identity Analytics Rare process execution in organization
Execution	Identity Analytics Rare process execution by user

Figure 8. QUIETCANARY's alerts shown in Cortex XDR.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: BrowserTelemetry
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 9. QUIETCANARY/Tunnus execution prevention alert shown in Cortex XDR.

Malware: Kopiluwak

Malware Type: Spreader/Downloader

First Seen: 2016

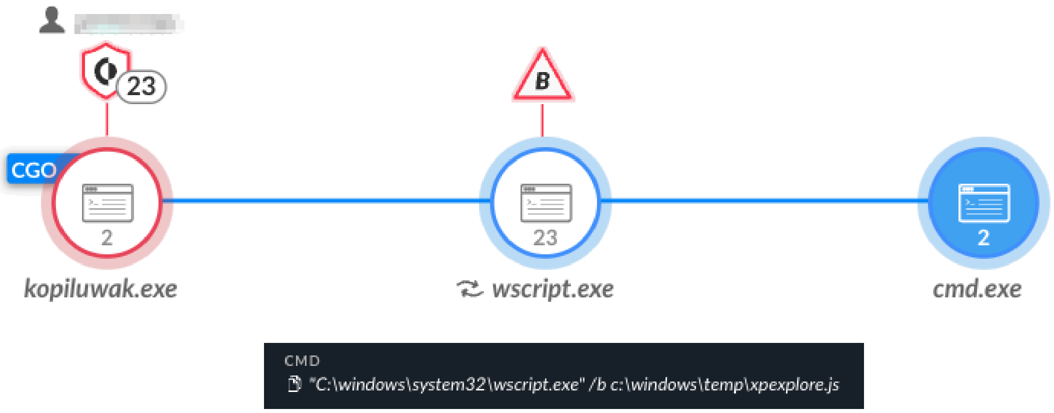
Description: Kopiluwak malware was discovered in late 2016, and it was delivered as a multilayered JavaScript payload by various types of droppers.

Pensive Ursa dropped the Kopiluwak malware using an MSIL dropper in 2017 in a G20-themed attack, and as an SFX executable in late 2022.

Kopiluwak's JavaScript file is depicted in Figure 10 and the code snippet below, dropped under the C:\Windows\Temp\ path. Its purpose is gathering valuable initial profiling information on the infected machine, such as the following:

- Listing files in strategic locations
- Retrieving the current running processes
- Displaying active network connections

The threat actor accomplished this activity by running reconnaissance commands such as systeminfo, tasklist, net, ipconfig, and dir. The results are saved in a file named result2.dat.

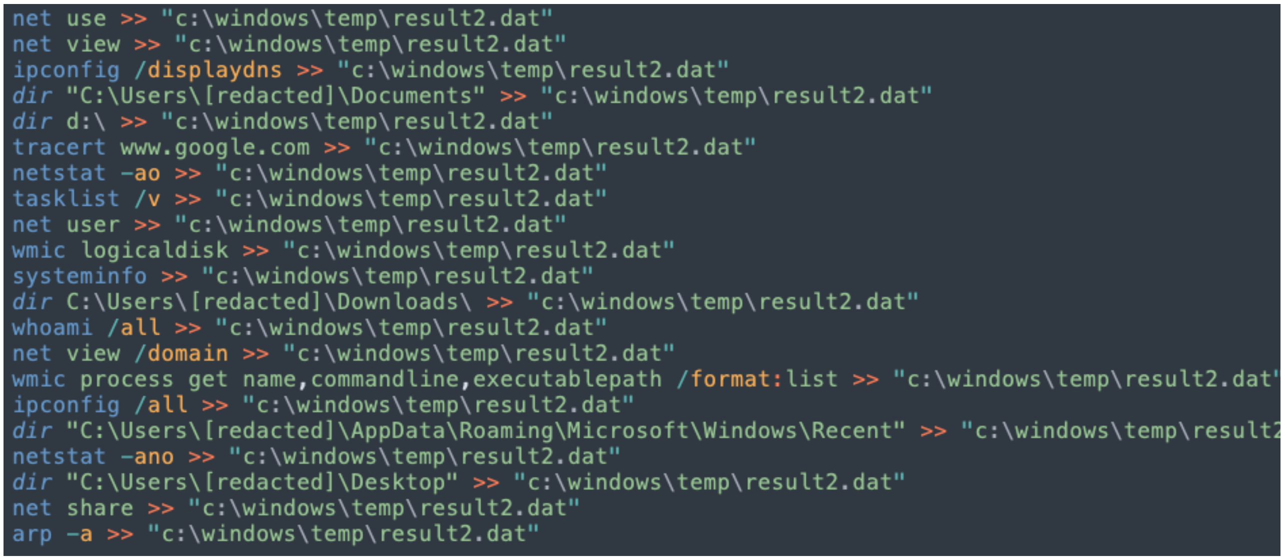


CMD

```
"C:\windows\system32\wscript.exe" /b c:\windows\temp\xpexplore.js
```

Figure 10. Kopiluwak execution detection as shown in Cortex XDR in detect mode.

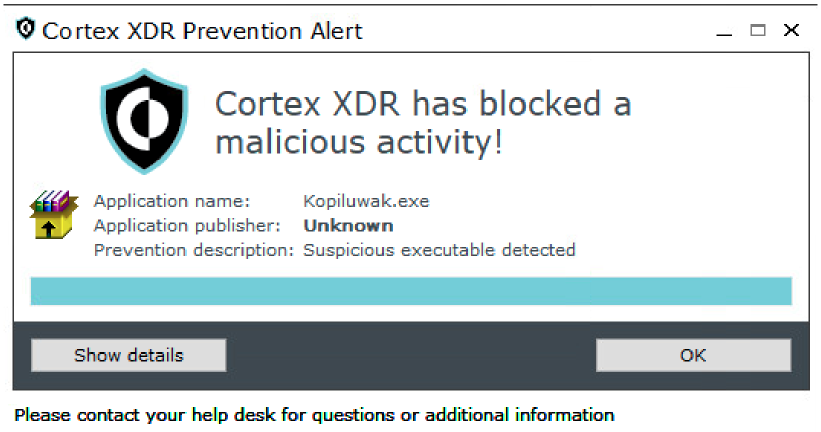
Listed in Figure 11 are the reconnaissance commands executed by Kopiluwak, and detected by Cortex XDR.



```
net use >> "c:\windows\temp\result2.dat"
net view >> "c:\windows\temp\result2.dat"
ipconfig /displaydns >> "c:\windows\temp\result2.dat"
dir "C:\Users\[redacted]\Documents" >> "c:\windows\temp\result2.dat"
dir d:\ >> "c:\windows\temp\result2.dat"
tracert www.google.com >> "c:\windows\temp\result2.dat"
netstat -ao >> "c:\windows\temp\result2.dat"
tasklist /v >> "c:\windows\temp\result2.dat"
net user >> "c:\windows\temp\result2.dat"
wmic logicaldisk >> "c:\windows\temp\result2.dat"
systeminfo >> "c:\windows\temp\result2.dat"
dir C:\Users\[redacted]\Downloads\ >> "c:\windows\temp\result2.dat"
whoami /all >> "c:\windows\temp\result2.dat"
net view /domain >> "c:\windows\temp\result2.dat"
wmic process get name,commandline,executablepath /format:list >> "c:\windows\temp\result2.dat"
ipconfig /all >> "c:\windows\temp\result2.dat"
dir "C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Recent" >> "c:\windows\temp\result2
netstat -ano >> "c:\windows\temp\result2.dat"
dir "C:\Users\[redacted]\Desktop" >> "c:\windows\temp\result2.dat"
net share >> "c:\windows\temp\result2.dat"
arp -a >> "c:\windows\temp\result2.dat"
```

Figure 11. Kopiluwak's reconnaissance commands.

Figure 12 shows Cortex XDR raising an execution prevention alert for Kopiluwak.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

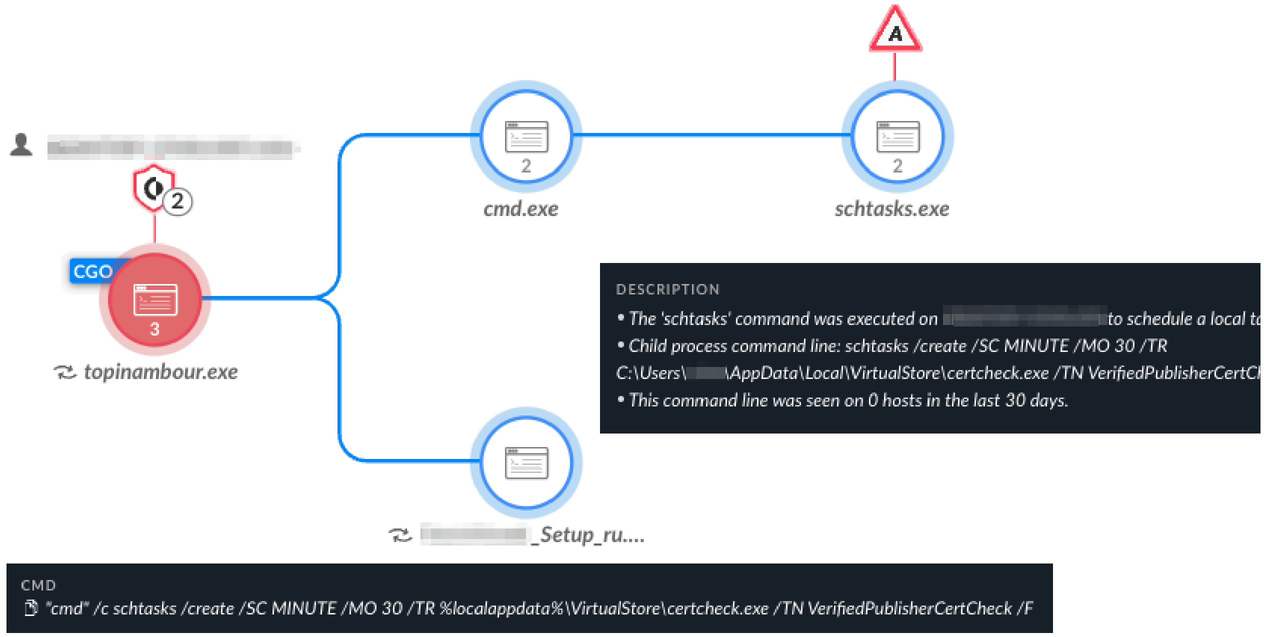
Application name: Kopiluwak.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 12. Kopiluwak execution prevention alert as shown in Cortex XDR.

In 2019, Pensive Ursa began to deliver Kopiluwak using the Topinambour dropper. The group bundled Topinambour into a legitimate software installer.

Upon installation, Topinambour is dropped as a small .NET file in the %localappdata% folder and written as a scheduled task, as shown in Figure 13. The malware then communicates with its hard-coded C2 virtual private server (VPS) to deliver the Kopiluwak malware.

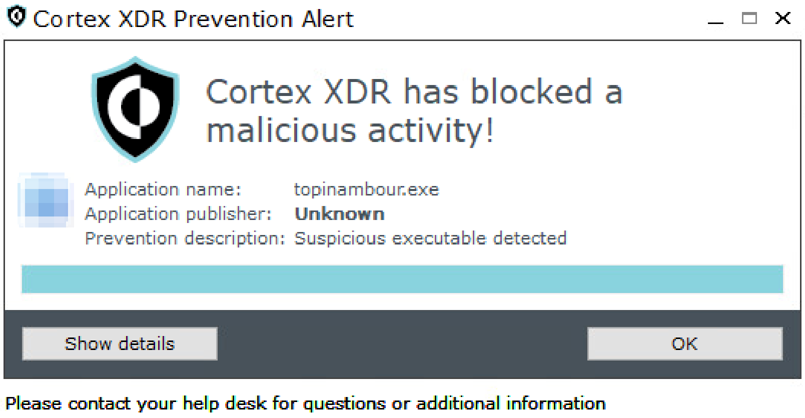


DESCRIPTION
- The 'schtasks' command was executed on [redacted] to schedule a local t
- Child process command line: schtasks /create /SC MINUTE /MO 30 /TR C:\Users\[redacted]\AppData\Local\VirtualStore\certcheck.exe /TN VerifiedPublisherCertC
- This command line was seen on 0 hosts in the last 30 days.

CMD
```
"cmd" /c schtasks /create /SC MINUTE /MO 30 /TR %localappdata%\VirtualStore\certcheck.exe /TN VerifiedPublisherCertCheck /F
```

Figure 13. Topinambour execution detection shown in Cortex XDR in detect mode.

Figure 14 shows the prevention alert pop-up raised by Cortex XDR.



Cortex XDR has blocked a malicious activity!

Application name: topinambour.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 14. Topinambour execution prevention alert shown in Cortex XDR.

Malware: Crutch

Malware Type: Backdoor

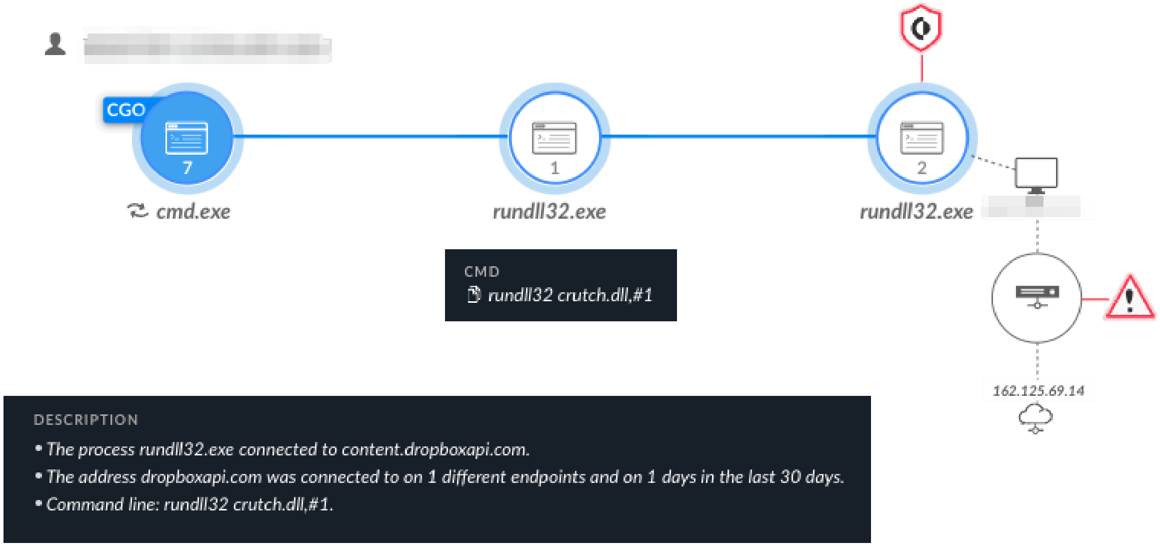
First Seen: 2015

Description: In December 2020, ESET researchers discovered the Crutch backdoor. In line with Pensive Ursa’s tactics, techniques and procedures (TTPs), the threat actor used the backdoor to attack a handful of targets in Europe, including the Ministry of Foreign Affairs of an EU member.

The main purpose of this backdoor was to eventually steal sensitive files and exfiltrate the data to a Dropbox account controlled by Pensive Ursa operators. Using commercial services such as Dropbox for C2 communication is a known (yet effective) technique due to it being a legitimate service, and blending in with other network communication.

This backdoor was attributed to Pensive Ursa due to strong similarities in code and TTPs with another backdoor from Pensive Ursa's arsenal called Gazer. Crutch is considered to be a second-stage backdoor, and its persistence is achieved using DLL hijacking.

Figures 15 and 16 show the detection and prevention of Crutch respectively, in Cortex XDR.

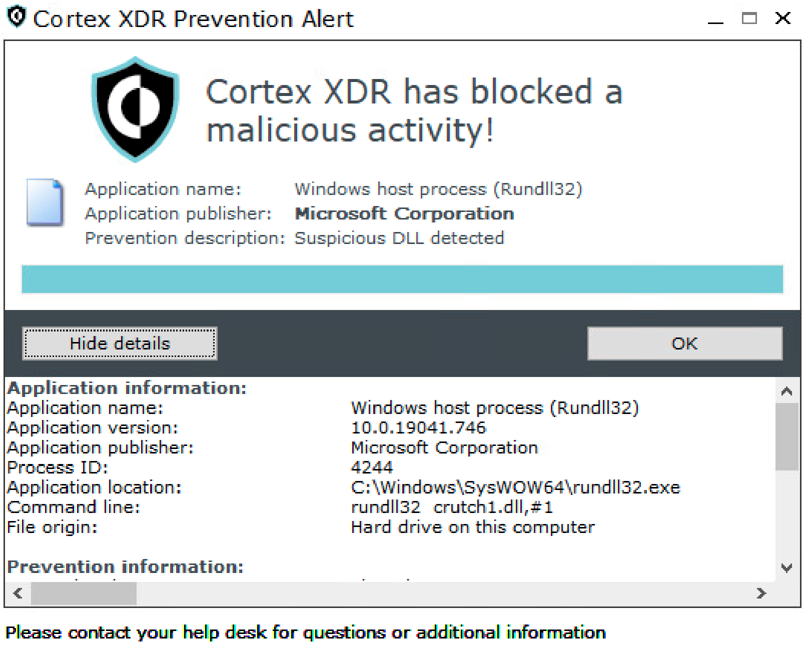


CMD
rundll32 crutch.dll,#1

DESCRIPTION

- The process rundll32.exe connected to content.dropboxapi.com.
- The address dropboxapi.com was connected to on 1 different endpoints and on 1 days in the last 30 days.
- Command line: rundll32 crutch.dll,#1.

Figure 15. Crutch execution detection shown in Cortex XDR in detect mode.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: Windows host process (Rundll32)
Application publisher: **Microsoft Corporation**
Prevention description: Suspicious DLL detected

Application information:

```
Application name:          Windows host process (Rundll32)
Application version:       10.0.19041.746
Application publisher:     Microsoft Corporation
Process ID:                4244
Application location:      C:\Windows\SysWOW64\rundll32.exe
Command line:              rundll32  crutch1.dll,#1
File origin:               Hard drive on this computer
```

Prevention information:

Please contact your help desk for questions or additional information

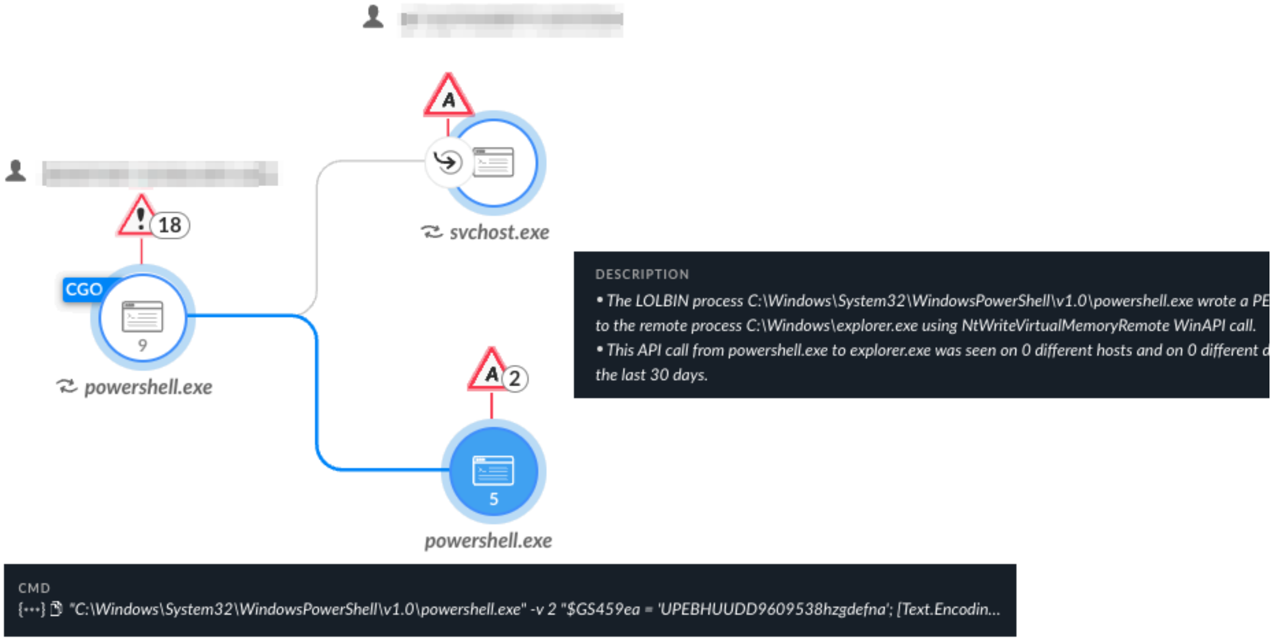
Figure 16. Crutch execution prevention alert shown in Cortex XDR.

Malware: ComRAT

Aliases: Agent.btz

Malware Type: Backdoor

First Seen: 2007

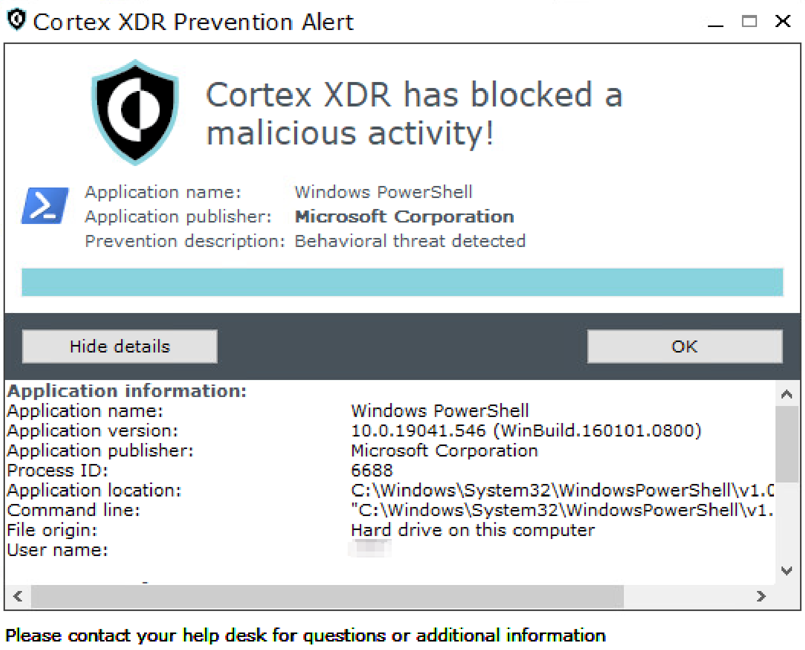


DESCRIPTION
• The LOLBIN process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe wrote a PE
to the remote process C:\Windows\explorer.exe using NtWriteVirtualMemoryRemote WinAPI call.
• This API call from powershell.exe to explorer.exe was seen on 0 different hosts and on 0 different d
the last 30 days.

CMD
```
{•••} "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -v 2 "$GS459ea = 'UPEBHUUDD9609538hzgdefna'; [Text.Encodin...
```

Figure 17. PowerShell dropper drops ComRAT to disk shown in Cortex XDR in detect mode.

Description: ComRAT is one of Pensive Ursa’s oldest backdoors, which they named Agent.btz in earlier iterations of the malware. ComRAT was reportedly first discovered in 2007. Since then it has had many upgrades. As of 2020, the latest iteration of ComRAT is version 4. This threat is developed in C++ and the threat actor has deployed it using PowerShell implants, such as PowerStallion. Figure 17 shows the PowerShell dropper mechanism. The threat actor’s main purpose of operations when using ComRAT was to steal and exfiltrate confidential documents from high value targets.



Cortex XDR has blocked a malicious activity!

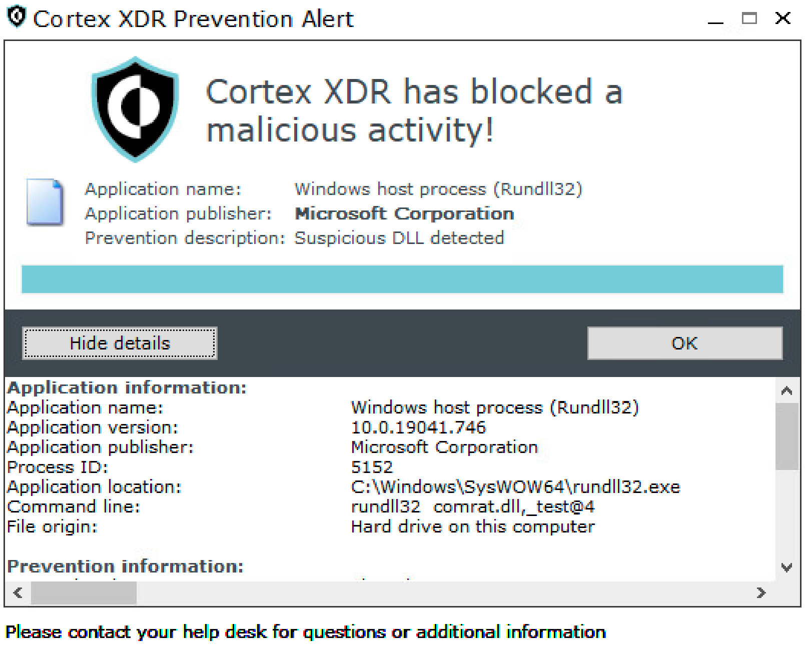
Application name: Windows PowerShell
Application publisher: **Microsoft Corporation**
Prevention description: Behavioral threat detected

```
Application information:
Application name:            Windows PowerShell
Application version:         10.0.19041.546 (WinBuild.160101.0800)
Application publisher:       Microsoft Corporation
Process ID:                  6688
Application location:        C:\Windows\System32\WindowsPowerShell\v1.0
Command line:                "C:\Windows\System32\WindowsPowerShell\v1.
File origin:                 Hard drive on this computer
User name:                   [redacted]
```

Please contact your help desk for questions or additional information

Figure 18a. ComRAT PowerShell dropper execution prevention alert shown in Cortex XDR.

Figures 18a and 18b depict the PowerShell and DLL executions preventions respectively, in Cortex XDR.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: Windows host process (Rundll32)
Application publisher: **Microsoft Corporation**
Prevention description: Suspicious DLL detected

Application information:

```
Application name:          Windows host process (Rundll32)
Application version:       10.0.19041.746
Application publisher:     Microsoft Corporation
Process ID:                5152
Application location:      C:\Windows\SysWOW64\rundll32.exe
Command line:              rundll32  comrat.dll,_test@4
File origin:               Hard drive on this computer
```

Prevention information:

Please contact your help desk for questions or additional information

Figure 18b. ComRAT DLL execution prevention alerts shown in Cortex XDR.

Malware: Carbon

Malware Type: Backdoor

First Seen: 2014

Description: Carbon is a modular backdoor framework that has been used by Pensive Ursa for several years. The Carbon framework includes an installer, an orchestrator component, a communication module and a configuration file.

Carbon also has P2P communication capabilities, which the threat actor uses to send commands to other infected machines on an affected network. Carbon receives commands from the C2 through the use of legitimate web services providers like Pastebin.

Figure 19 and Figure 20 show Carbon's execution detection and prevention in Cortex XDR.

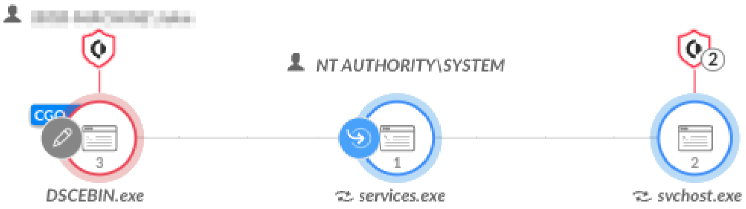
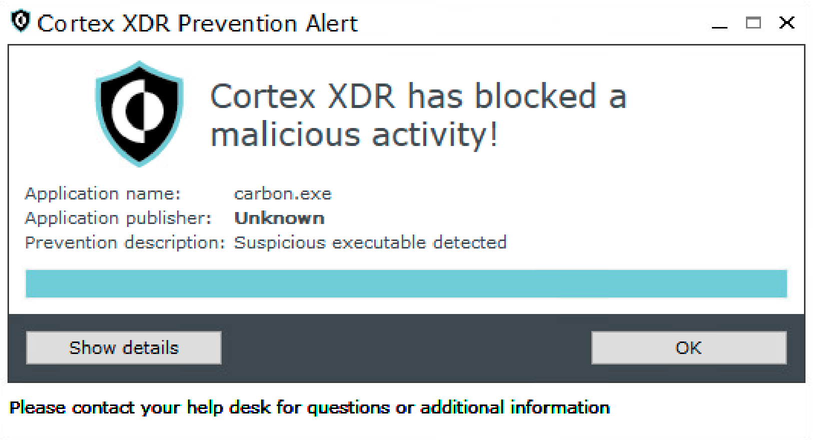


Figure 19. Carbon creates a service that loads the additional components, which is shown in Cortex XDR in detect mode.


Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: carbon.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 20. Carbon execution prevention alert shown in Cortex XDR.

Malware: HyperStack

Malware Type: Backdoor

First Seen: 2018

Description: HyperStack (aka SilentMoo, BigBoss) is an RPC backdoor that was first observed in 2018, which the threat actor used in operations targeting government entities in Europe. HyperStack operates with a controller that uses named pipes to communicate over RPC with other machines in a compromised environment that are infected with HyperStack. This communication method enables the attacker to control machines on a local network.

HyperStack shows several similarities with Pensive Ursa's Carbon backdoor, such as the encryption scheme, configuration file format and logging convention.

Figure 21 and Figure 22 show HyperStack's detection and prevention respectively, in Cortex XDR.

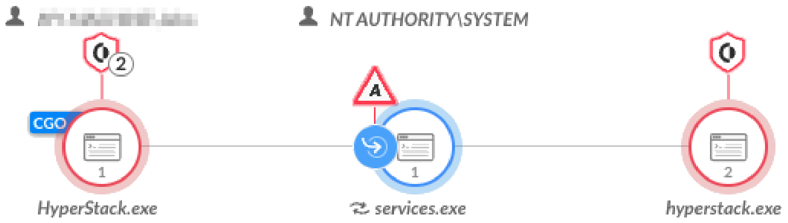
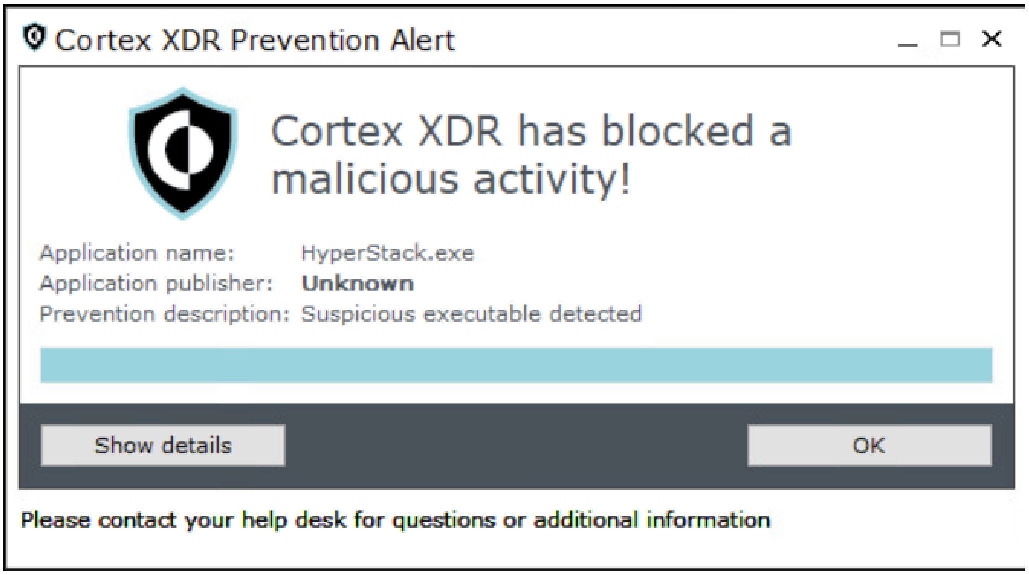


Figure 21. HyperStack creates a service for persistence shown in Cortex XDR in detect mode.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: HyperStack.exe
Application publisher: **Unknown**
Prevention description: Suspicious executable detected

Please contact your help desk for questions or additional information

Figure 22. HyperStack execution prevention alert shown in Cortex XDR.

Malware: TinyTurla

Malware Type: Backdoor

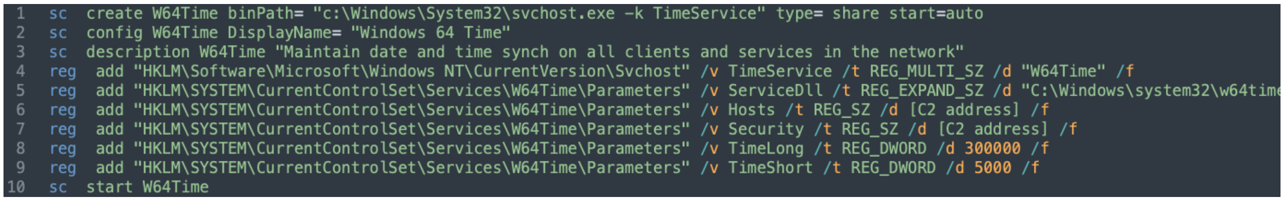
First Seen: 2021

Description: The TinyTurla malware was first discovered by Talos in 2021. They assumed it was a second stage backdoor, and it has been seen on targets in the US, EU and later in Asia.

TinyTurla's main features include the following:

- Downloading additional payloads
- Uploading files to the attacker's C2 server
- Executing other processes

As shown in Figure 23, threat actors install the backdoor via a batch script as a service called Windows Time Service. The batch script is also in charge of writing the C2 server's data to the registry. Once the backdoor is executed, it reads these values to communicate with its C2. It masquerades as a DLL called w64time.dll, under the system32 folder.

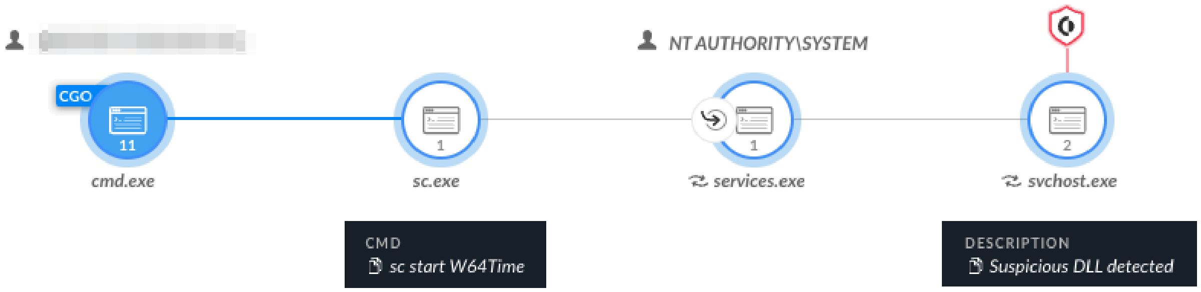


```
sc  create W64Time binPath= "c:\Windows\System32\svchost.exe -k TimeService" type= share start=auto
sc  config W64Time DisplayName= "Windows 64 Time"
sc  description W64Time "Maintain date and time synch on all clients and services in the network"
reg  add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Svchost" /v TimeService /t REG_MULTI_SZ /d "W64Time" /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\W64Time\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\system32\w64time
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\W64Time\Parameters" /v Hosts /t REG_SZ /d [C2 address] /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\W64Time\Parameters" /v Security /t REG_SZ /d [C2 address] /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\W64Time\Parameters" /v TimeLong /t REG_DWORD /d 300000 /f
reg  add "HKLM\SYSTEM\CurrentControlSet\Services\W64Time\Parameters" /v TimeShort /t REG_DWORD /d 5000 /f
sc  start W64Time
```

Figure 23. Content of the batch script described above.

Although w32time.dll is a legitimate DLL, and other legitimate DLLs do have both 32- and 64-bit variants, a legitimate w64time.dll does not exist. This naming convention is intended to further distract victims from suspecting anything is amiss.

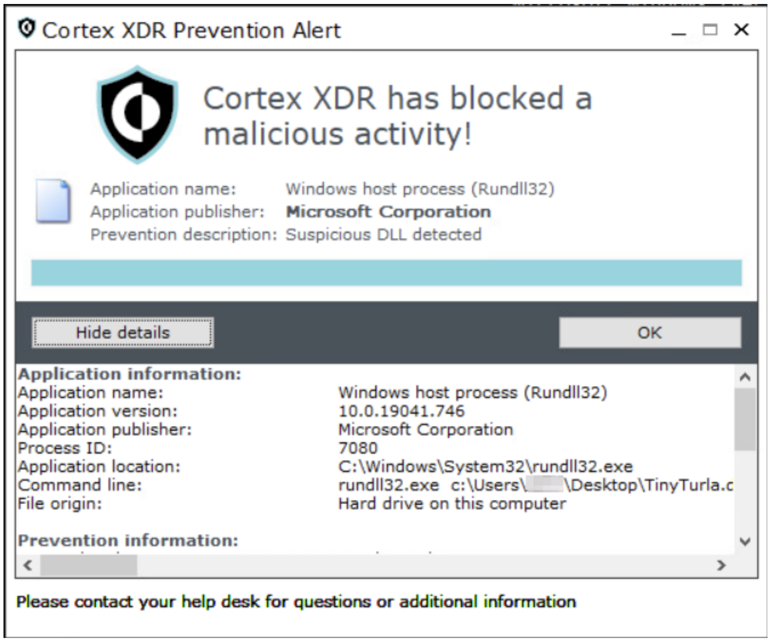
Figure 24 and Figure 25 show Cortex XDR detecting the writing and execution of the batch script, the W64Time service and the TinyTurla DLL execution.



CMD
sc start W64Time

DESCRIPTION
Suspicious DLL detected

Figure 24. TinyTurla prevention shown in Cortex XDR in detect mode.



Cortex XDR Prevention Alert

Cortex XDR has blocked a malicious activity!

Application name: Windows host process (Rundll32)
Application publisher: **Microsoft Corporation**
Prevention description: Suspicious DLL detected

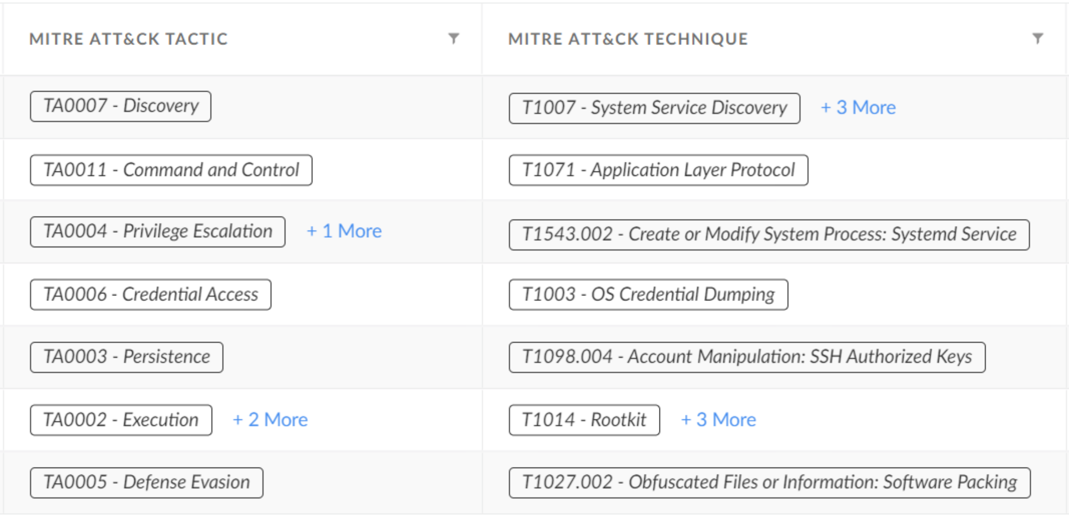
```
Application information:
Application name:          Windows host process (Rundll32)
Application version:       10.0.19041.746
Application publisher:     Microsoft Corporation
Process ID:                7080
Application location:      C:\Windows\System32\rundll32.exe
Command line:              rundll32.exe  c:\Users\[redacted]\Desktop\TinyTurla.c
File origin:               Hard drive on this computer

Prevention information:
```

Please contact your help desk for questions or additional information

Figure 25. TinyTurla execution prevention alert shown in Cortex XDR.

Tactics, Techniques and Procedures (TTPs)

Cortex XDR alerts are mapped to the MITRE ATT&CK framework and present information about the tactic and the technique associated with the threat, as shown in Figure 26 below.



MITRE ATT&CK TACTIC	MITRE ATT&CK TECHNIQUE
TA0007 - Discovery	T1007 - System Service Discovery + 3 More
TA0011 - Command and Control	T1071 - Application Layer Protocol
TA0004 - Privilege Escalation + 1 More	T1543.002 - Create or Modify System Process: Systemd Service
TA0006 - Credential Access	T1003 - OS Credential Dumping
TA0003 - Persistence	T1098.004 - Account Manipulation: SSH Authorized Keys
TA0002 - Execution + 2 More	T1014 - Rootkit + 3 More
TA0005 - Defense Evasion	T1027.002 - Obfuscated Files or Information: Software Packing

Figure 26. Mitre ATT&CK mapping in Cortex XDR.

Pensive Ursa-related activities and arsenal raised multiple alerts in Cortex XDR, which were mapped to the MITRE ATT&CK tactics and techniques referenced in Table 1.

MITRE ATT&CK tactic	MITRE ATT&CK technique
Resource Development	Acquire Infrastructure, Compromise Infrastructure, Develop Capabilities, Obtain Capabilities
Execution	Command and Scripting Interpreter, Native API, User Execution
Initial Access	Drive-by Compromise, Phishing, Valid Accounts
Persistence	Boot or Logon Autostart Execution, Event Triggered Execution, Valid Accounts
Privilege Escalation	Access Token Manipulation, Boot or Logon Autostart Execution, Event Triggered Execution, Exploitation for Privilege Escalation, Process Injection, Valid Accounts
Defense Evasion	Access Token Manipulation, Deobfuscate/Decode Files or Information, Impair Defenses, Modify Registry, Obfuscated Files or Information, Process Injection, Subvert Trust Controls, Valid Accounts
Credential Access	Brute Force, Credentials from Password Stores
Discovery	Account Discovery, File and Directory Discovery, Group Policy Discovery, Password Policy Discovery, Peripheral Device Discovery, Permission Groups Discovery, Process Discovery, Query Registry, Remote System Discovery, Software Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery
Lateral Movement	Lateral Tool Transfer, Remote Services
Collection	Archive Collected Data, Data from Information Repositories, Data from Local System, Data from Removable Media
Command and Control	Application Layer Protocol, Ingress Tool Transfer, Proxy, Web Service
Exfiltration	Exfiltration Over Web Service

Table 1. MITRE ATT&CK tactics and techniques.

Conclusion

The Pensive Ursa advanced persistent threat (APT) group is known to be a significant and persistent adversary. With their advanced techniques, this Russian-FSB operated group has demonstrated an evasive modus operandi while targeting a wide range of sectors across the globe.

We explored the top 10 types of malware in Pensive Ursa's arsenal and witnessed their execution through the lens of Palo Alto Networks Cortex XDR product. This demonstrated the importance of using a multilayered protection model against an advanced threat.

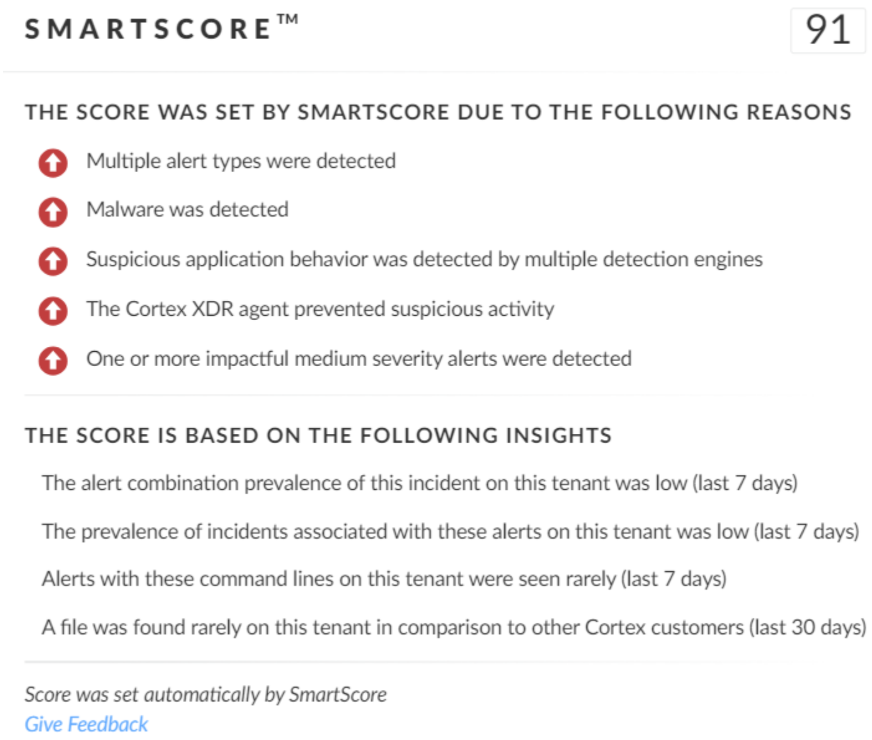
The potential damage of falling victim to a Pensive Ursa APT attack can be significant. The consequences extend beyond financial losses and data breaches to the possibility of them reaching critical infrastructure, which could have national security and geopolitical ramifications. Thus, every organization, regardless of its size or industry, must prioritize comprehensive security strategies and invest in multilayer security measurements to safeguard against the growing threat of APT groups like Pensive Ursa.

Protections and Mitigations

Palo Alto Networks Cortex XDR and XSIAM customers receive protections against Pensive Ursa's arsenal of malware described in this blog post.

Prevention and detection alerts were raised for each malware: Capibar, Kazua, Snake, Kopiluwak, QUIETCANARY/Tunnus, Crutch, ComRAT, Carbon, HyperStack and TinyTurla.

SmartScore is a unique ML-driven scoring engine that translates security investigation methods and their associated data into a hybrid scoring system. It scored an incident involving a combination of known Pensive Ursa tools and techniques a 91 score, which is a very high level of risk, as shown below in Figure 26.



SMARTSCORE™ 91

THE SCORE WAS SET BY SMARTSCORE DUE TO THE FOLLOWING REASONS

- ⬆ Multiple alert types were detected
- ⬆ Malware was detected
- ⬆ Suspicious application behavior was detected by multiple detection engines
- ⬆ The Cortex XDR agent prevented suspicious activity
- ⬆ One or more impactful medium severity alerts were detected

THE SCORE IS BASED ON THE FOLLOWING INSIGHTS

The alert combination prevalence of this incident on this tenant was low (last 7 days)

The prevalence of incidents associated with these alerts on this tenant was low (last 7 days)

Alerts with these command lines on this tenant were seen rarely (last 7 days)

A file was found rarely on this tenant in comparison to other Cortex customers (last 30 days)

Score was set automatically by SmartScore
Give Feedback

Figure 27. SmartScore information about the incident.

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

Cortex XDR detects user and credential-based threats by analyzing user activity from multiple data sources including the following:

- Endpoints
- Network firewalls
- Active Directory
- Identity and access management solutions
- Cloud workloads

Cortex XDR builds behavioral profiles of user activity over time with machine learning. By comparing new activity to past activity, peer activity and the expected behavior of the entity, Cortex XDR detects anomalous activity indicative of credential-based attacks.

It also offers the following protections related to the attacks discussed in this post:

- Prevents the execution of known malicious malware and also prevents the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module
- Protects against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4
- Protects from threat actors dropping and executing commands from web shells using Anti-Webshell Protection, newly released in Cortex XDR 3.4
- Protects against exploitation of different vulnerabilities including ProxyShell and ProxyLogon using the Anti-Exploitation modules as well as Behavioral Threat Protection
- Cortex XDR Pro detects post-exploit activity, including credential-based attacks, with behavioral analytics

If you think you might have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

North America Toll-Free: 866.486.4842 (866.4.UNIT42)

- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Capibar

Hashes (SHA-256):

- ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39
- 64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a

Domains:

- hxxps://mail.numina[.]md/owa/scripts/logon.aspx
- hxxps://mail.aet.in[.]ua/outlook/api/logoff.aspx
- hxxps://mail.arlingtonhousing[.]us/outlook/api/logoff.aspx
- hxxps://mail.kzp[.]bg/outlook/api/logoff.aspx
- hxxps://mail.lechateaudelatour[.]fr/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITC
- hxxps://mail.lebsack[.]de/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SY

Kazuar

Hashes (SHA-256):

- 8490daab736aa638b500b27c962a8250bbb8615ae1c68ef77494875ac9d2ada2
- b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70
- Bf6f30673cf771d52d589865675a293dc5c3668a956d0c2fc0d9403424d429b2
- cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858

Domains:

- Gaismustudija[.]lv
- Hcdh-tunisie[.]org
- www.gallen[.]fi
- hxxps://www.bombheros[.]com/wp-content/languages/index[.]php
- hxxps://www.simplifiedhomesales[.]com/wp-includes/images/index.php
- hxxp://mtsoft.hol[.]es/wp-content/gallery/
- hxxp://www.polishpod101[.]com/forum/language/en/sign/
- hxxps://www.pierreagencement[.]fr/wp-content/languages/index.php
- hxxps://sansaispa[.]com/wp-includes/images/gallery/
- hxxps://octoberoctopus.co[.]za/wp-includes/sitemaps/web/

Snake

Hashes (SHA-256):

- fc68026b83392aa227e9adf9c71289cb51ba03427f6de67a73ae872e19ef6ff9
- 1950d2e706fbc6263d376c0c4f16bd5acfd543248ee072657ba3dd62da8427eb
- cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986
- b262292e049ee75d235164df98fa8ed09a9e2a30c5432623856bafd4bd44d801

Kopiluwak

Hashes (SHA-256):

- 6536b6b50aa1f6899ffa90aaf4b1b67c0ae0f6c0441016f5308b37c12141c61d
- 8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3

Domains:

- manager.surro[.]am

IPs:

- 194.67.209[.]186

Topinambour

Hashes (SHA-256):

- 009406c1c7c0b289a25d44dfaa8364633d9b71df5f3c7a65deec1ef00a8c2ebb
- 7a7d11adbcb740323eb52b097f535cfa5c281bf07a4d5c4afb0c5182fa4ffd1b
- d4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71
- 046f11a6c561e46e6bf199ab7f50e74a4d2aaead68cdbd6ce44b37b5b4964758

IPs:

- 197.168.0[.]247

QUIETCANARY/Tunnus

Hashes (SHA-256):

- 0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852
- 3f94b20cb7f4ff55207660649ebbb02679c991fe03efbcb0bd3840fc7f0bd527
- 29314f3cd73b81eda7bd90c66f659235e6bb900e499c9cc7057d10a9083a0b94
- 87663affd147065d08d4fe76d9a18b0d7d85fab68cf9f5ac96cfdfff3f27ffd2

Domains:

- lakihelppi[.]com

IPs:

- 46.101.209[.]249
- 210.48.231[.]182

Crutch

Hashes (SHA-256):

- 0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5
- 29b1da7b17a7ba3e730e6927058d0554a8bc81bdef88e364097fab0bb1950edc
- 16860fc685ea0dee91e65e253062153ac6c886fdd73a3020c266601f58038a61
- 10c0e2afb37a24ac7732a402a4c9d854b35a382f1651d4aa2ece429b154aecb2

ComRAT

Hashes (SHA-256):

- 00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d
- 134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8
- 166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405
- 44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316
- A3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642
- 187bf95439da038c1bc291619507ff5e426d250709fa5e3eda7fda99e1c9854c
- b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4

Domains:

- branter[.]tk
- wekanda[.]tk
- sanitar[.]ml
- duke6[.]tk
- bronerg[.]tk
- Crusider[.]tk

Carbon

Hashes (SHA-256):

- 493e5fae191950b901764868b065ddddffa4f4c9b497022ee2f998b4a94f0fc2
- f3aaa091fdbc8772fb7bd3a81665f4d33c3b62bf98caad6fee4424654ba26429
- 2b969111dd1968d47b02d6390c92fb622cd03570b02ecf9215031ff03611a2b7
- 7d5794ad91351c7c5d7fbad8e83e3b71a09baac65fb09ca75d8d18339d24a46f

Domains:

- www.berlinguas[.]com
- www.balletmaniacs[.]com

HyperStack

Hashes (SHA-256):

- 6ca0b4efe077fe05b2ae871bf50133c706c7090a54d2c3536a6c86ff454caa9a
- 20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5
- e33580ae3df9d27d7cfb7b8f518a2704e55c92dd74cbbab8ef58ddfd36524cc8

TinyTurla

Hashes (SHA-256):

- 030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01