Void Rabisu’s Use of RomCom Backdoor Shows a Growing Shift in Threat Actors’ Goals

trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

May 30, 2023

Cyber Threats

Void Rabisu, a malicious actor believed to be associated with the RomCom backdoor, was thought to be driven by financial gain because of its ransomware attacks. But in this blog entry, we discuss how the use of the RomCom backdoor in recent attacks shows how Void Rabisu's motives seem to have changed since at least October 2022.

By: Feike Hacquebord, Stephen Hilt, Fernando Merces, Lord Alfred Remorin May 30, 2023
Read time: (words)

With contributions from Veronica Chierzi and Jayvee Mark Villaroman

Since the start of the war in Ukraine in February 2022, the number of cyber campaigns against Ukraine and North Atlantic Treaty Organization (NATO) countries has increased significantly. These campaigns come from many different angles: known advanced persistent threat (APT) actors, APT actors that were not publicly reported on before, and cyber mercenaries, hacktivists, and criminal actors who appear to have shifted from purely financial motives to geopolitical goals. In the past, these actors had different motivations, mode of operations, and targets, but the line between their campaigns has started to blur: Not only is an overlap in their targeting becoming apparent, but the distinction between their modes of operation is less clear. For instance, in 2022, one of Conti’s affiliates was found to be using its initial access techniques against Ukraine instead of using them to spread ransomware.

Another example of this is Void Rabisu, also known as Tropical Scorpius, an actor believed to be associated with Cuba ransomware and the RomCom backdoor. Because of its many ransomware attacks, Void Rabisu was believed to be financially motivated, even though its associated Cuba ransomware allegedly attacked the parliament of Montenegro in August 2022, which could be considered part of a geopolitical agenda. The motives of Void Rabisu seem to have changed since at least October 2022, when Void Rabisu’s associated RomCom backdoor was reported to have been used in attacks against the Ukrainian government and military: In a campaign in December 2022, a fake version of the Ukrainian army’s DELTA situational awareness website was used to lure targets into installing the RomCom backdoor. Normally, this kind of brazen attack would be thought to be the work of a nation state-sponsored actor, but in this case, the indicators clearly pointed towards Void Rabisu, and some of the tactics, techniques, and procedures (TTPs) used were typically associated with cybercrime.

Trend Micro’s telemetry and research corroborates that the RomCom backdoor has been used in geopolitically motivated attacks since at least October 2022, with targets that included organizations in Ukraine’s energy and water utility sectors. Targets outside of Ukraine were observed as well, such as a provincial local government that provides help to Ukrainian refugees, a parliament member of a European country, a European defense company, and various IT service providers in Europe and the US. Independent research from Google showed that RomCom was being used in campaigns against attendees of the Masters of Digital conference, a conference organized by DIGITALEUROPE, and the Munich Security Conference.

In this blog entry, we will discuss how the use of the RomCom backdoor fits into the current landscape, where politically motivated attacks are not committed by nation-state actors alone. Even though we cannot confirm coordination between the different attacks, Ukraine and countries who support Ukraine are being targeted by various actors, like APT actors, hacktivists, cyber mercenaries, and cybercriminals like Void Rabisu. We will also delve into how RomCom has evolved over time and how the backdoor is spread both by methods that look like APT, as well as methods used by prominent cybercriminal campaigns taking place currently, to show that RomCom is using more detection evasion techniques that are popular among the most impactful cybercriminals.

We assess that RomCom makes use of the same third-party services that are being utilized by other criminal actors as well, like malware signing and binary encryption. RomCom has been spread through numerous lure sites that are sometimes set up in rapid bursts. These lure sites are most likely only meant for a small number of targets, thus making discovery and analysis more difficult. Void Rabisu is one of the most evident examples of financially motivated threat actors whose goals and motivations are becoming more aligned under extraordinary geopolitical circumstances, and we anticipate that this will happen more in the future.

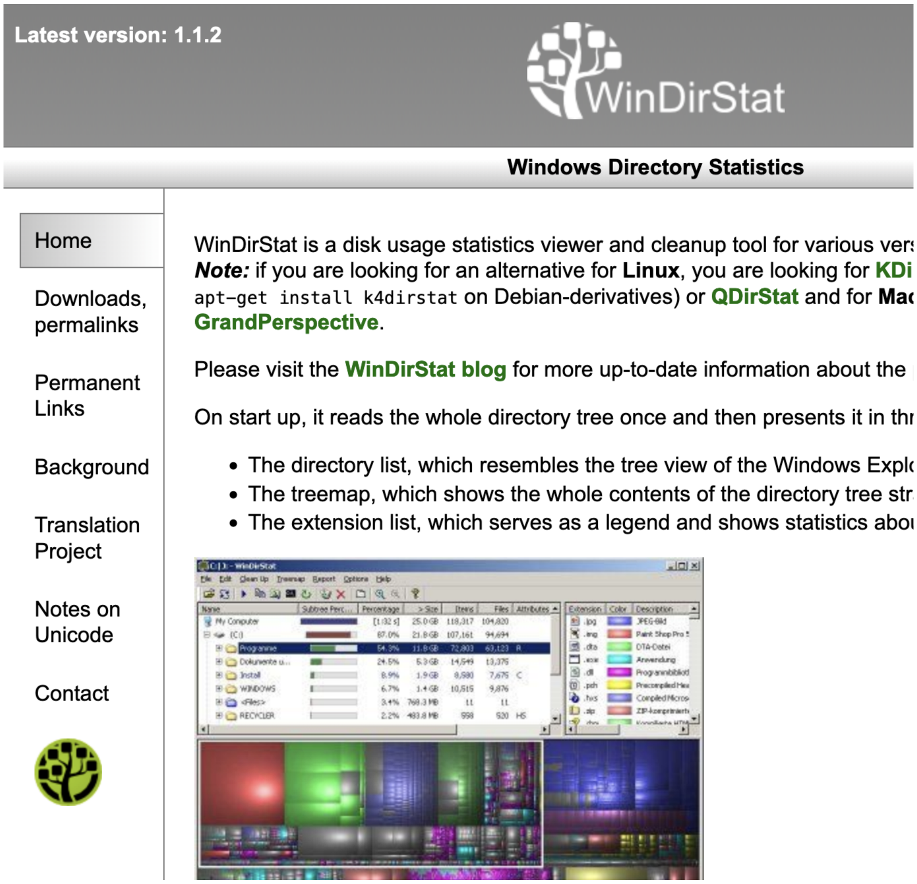
RomCom campaigns

We have been tracking RomCom campaigns since the summer of 2022, and since then, have seen an escalation in its detection evasion methods: Not only do the malware samples routinely use VMProtect to make both manual and automated sandbox analysis more difficult, they also utilize binary padding techniques on the payload files. This adds a significant amount of overlay bytes to the files, increasing the size of the malicious payload (we've seen a file with 1.7 gigabytes). Additionally, a new routine has been recently added that involves the encryption of the payload files, which can only be decrypted if a certain key is downloaded to activate the payload.

In addition to these technical evasion techniques, RomCom is being distributed using lure sites that often appear legitimate and are being utilized in narrow targeting. This makes automated blocking of these lure websites through web reputation systems harder. Void Rabisu has been using Google Ads to entice their targets to visit the lure sites, similar to a campaign that distributed IcedID botnet in December 2022. A key difference is that while IcedID's targeting was wider, Void Rabisu probably opted for narrower targeting that Google Ads offers to its advertisers. RomCom campaigns also make use of highly targeted spear phishing emails.

On the RomCom lure sites, targets are offered trojanized versions of legitimate applications, like chat apps such as AstraChat and Signal, PDF readers, remote desktop apps, password managers, and other tools, that are typically used by system administrators.

dirwinstat.com
(as of April 4, 2023)



Latest version: 1.1.2

Windows Directory Statistics

- Home
- Downloads, permalinks
- Permanent Links
- Background
- Translation Project
- Notes on Unicode
- Contact

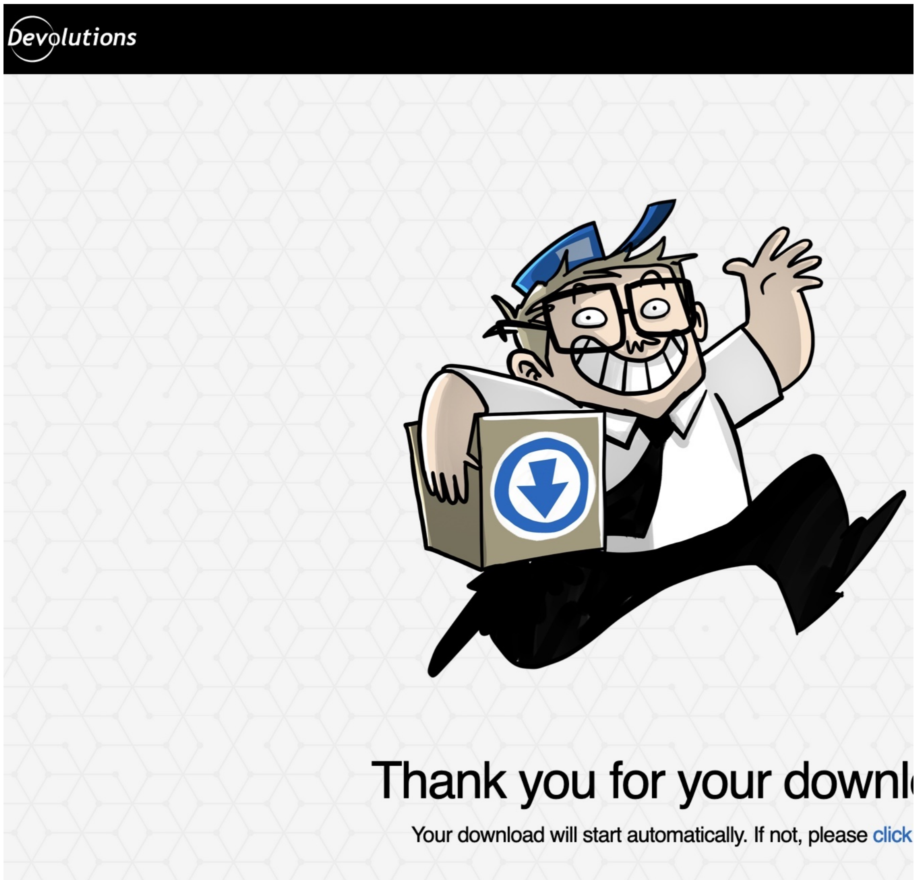
WinDirStat is a disk usage statistics viewer and cleanup tool for various vers
Note: if you are looking for an alternative for **Linux**, you are looking for **KDi**
`apt-get install k4dirstat` on Debian-derivatives) or **QDirStat** and for **Mac**
GrandPerspective.

Please visit the **WinDirStat blog** for more up-to-date information about the

On start up, it reads the whole directory tree once and then presents it in thr

- The directory list, which resembles the tree view of the Windows Explo
- The treemap, which shows the whole contents of the directory tree str
- The extension list, which serves as a legend and shows statistics abou

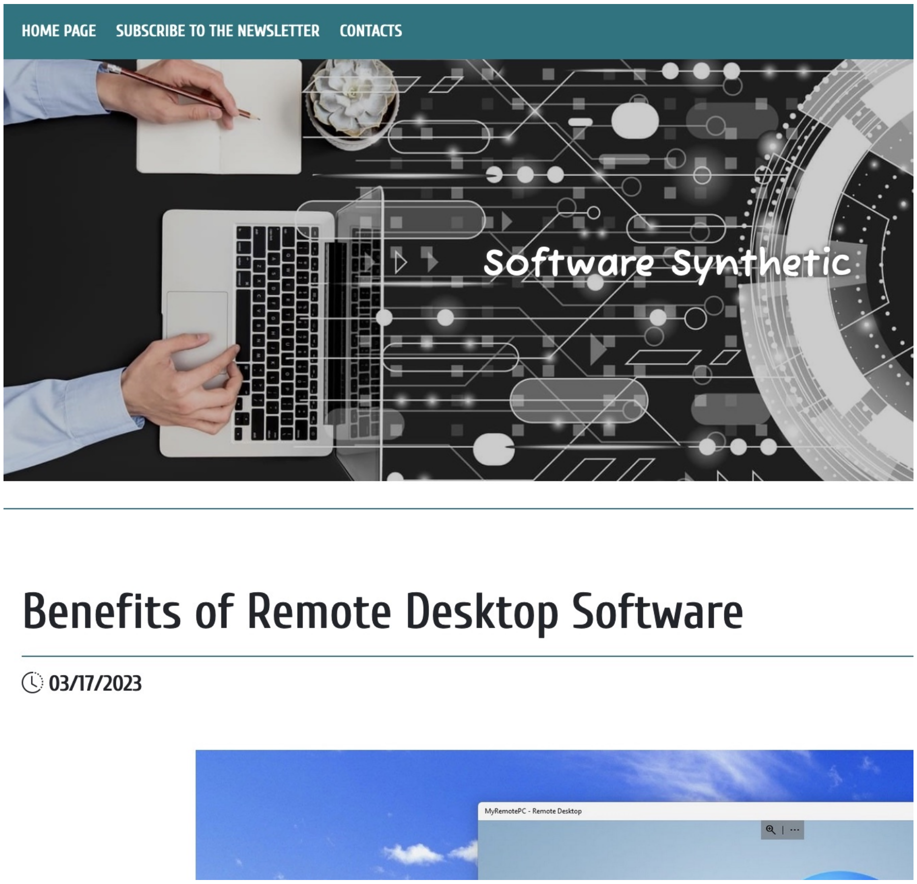
devolrdm.com
(as of March 23, 2023)



Thank you for your downl

Your download will start automatically. If not, please click

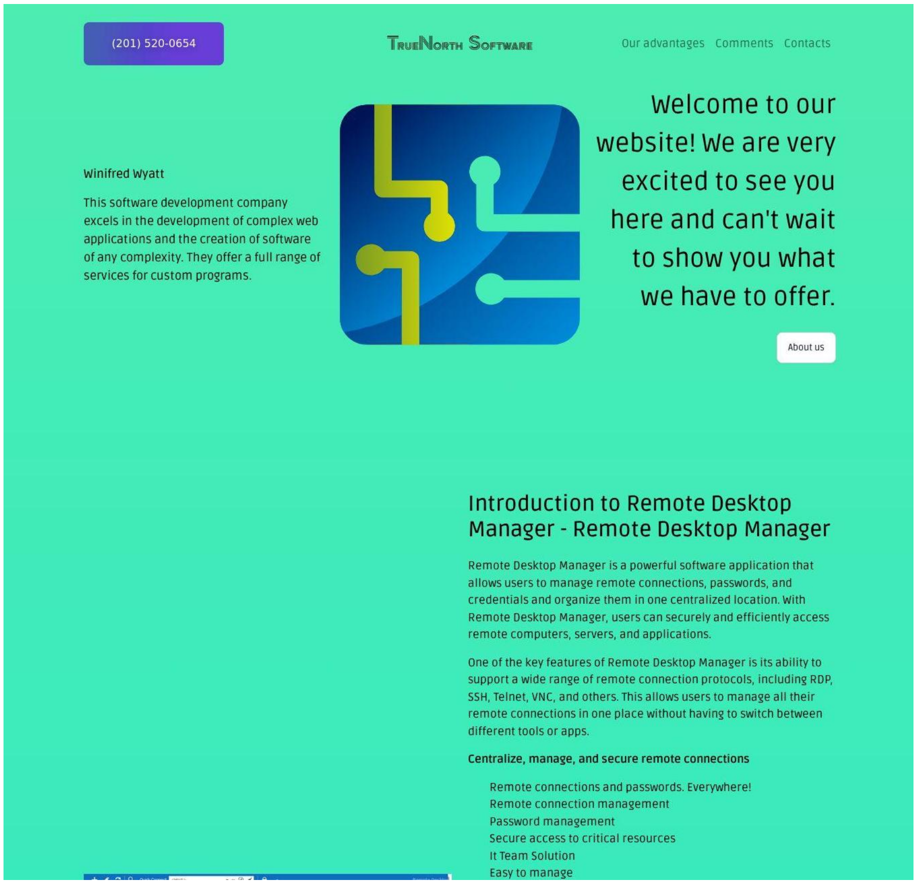
vectordmanagesoft.com
(as of March 22, 2023)



Benefits of Remote Desktop Software

03/17/2023

cozy-sofware.com
(as of March 13, 2023)



(201) 520-0654

TrueNorth Software

Our advantages Comments Contacts

Winifred Wyatt

This software development company excels in the development of complex web applications and the creation of software of any complexity. They offer a full range of services for custom programs.

Welcome to our website! We are very excited to see you here and can't wait to show you what we have to offer.

About us

Introduction to Remote Desktop Manager - Remote Desktop Manager

Remote Desktop Manager is a powerful software application that allows users to manage remote connections, passwords, and credentials and organize them in one centralized location. With Remote Desktop Manager, users can securely and efficiently access remote computers, servers, and applications.

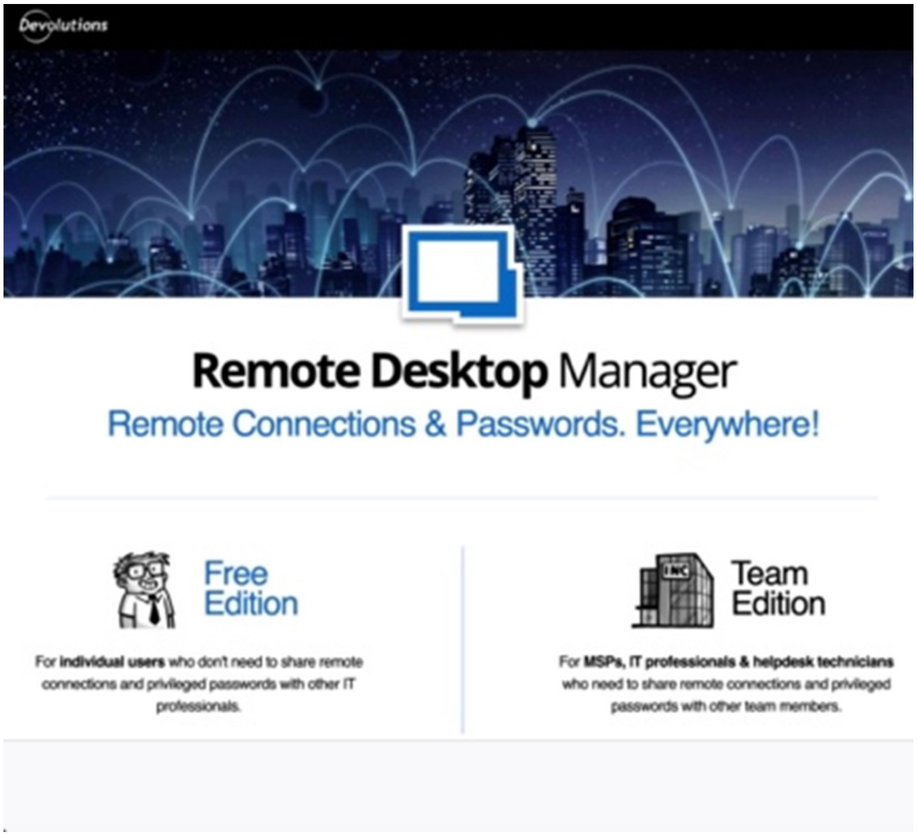
One of the key features of Remote Desktop Manager is its ability to support a wide range of remote connection protocols, including RDP, SSH, Telnet, VNC, and others. This allows users to manage all their remote connections in one place without having to switch between different tools or apps.

Centralize, manage, and secure remote connections

Remote connections and passwords. Everywhere!
Remote connection management
Password management
Secure access to critical resources
It Team Solution
Easy to manage

devolutionrdp.com

(as of March 6, 2023)



Devolutions

Remote Desktop Manager
Remote Connections & Passwords. Everywhere!

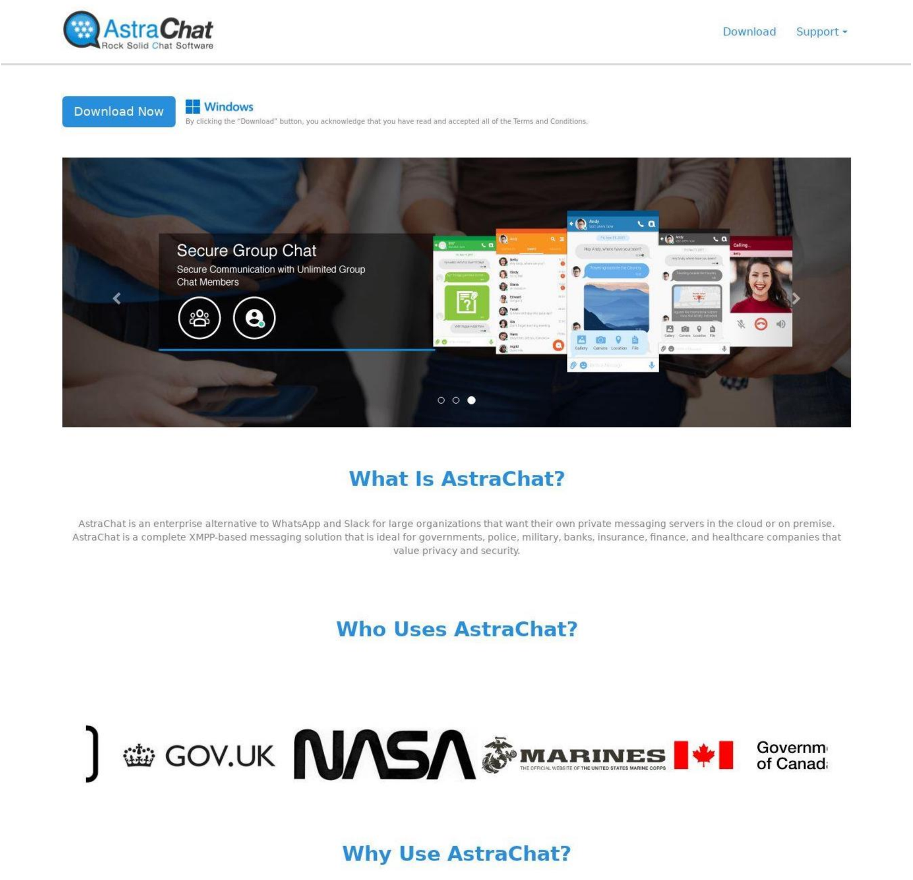
Free Edition

For **individual users** who don't need to share remote connections and privileged passwords with other IT professionals.

Team Edition

For **MSPs, IT professionals & helpdesk technicians** who need to share remote connections and privileged passwords with other team members.

astrachats.com
(as of February 27, 2023)



By clicking the "Download" button, you acknowledge that you have read and accepted all of the Terms and Conditions.

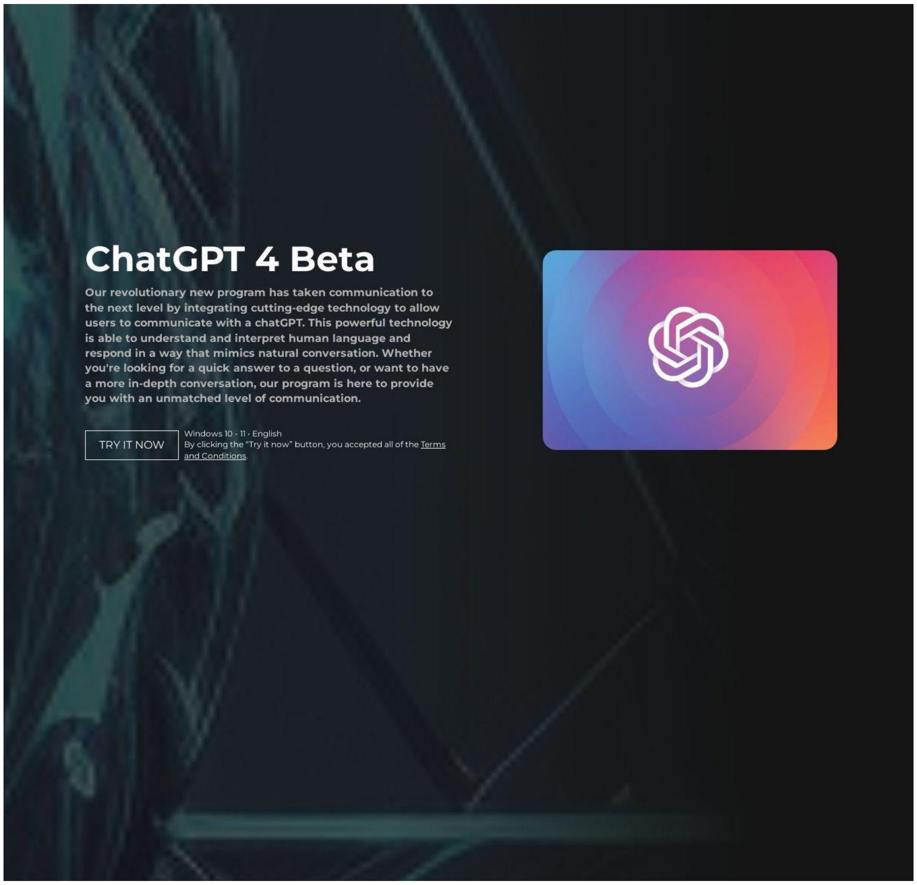
What Is AstraChat?

AstraChat is an enterprise alternative to WhatsApp and Slack for large organizations that want their own private messaging servers in the cloud or on premise. AstraChat is a complete XMPP-based messaging solution that is ideal for governments, police, military, banks, insurance, finance, and healthcare companies that value privacy and security.

Who Uses AstraChat?

Why Use AstraChat?

chatgpt4beta.com
(as of February 23, 2023)

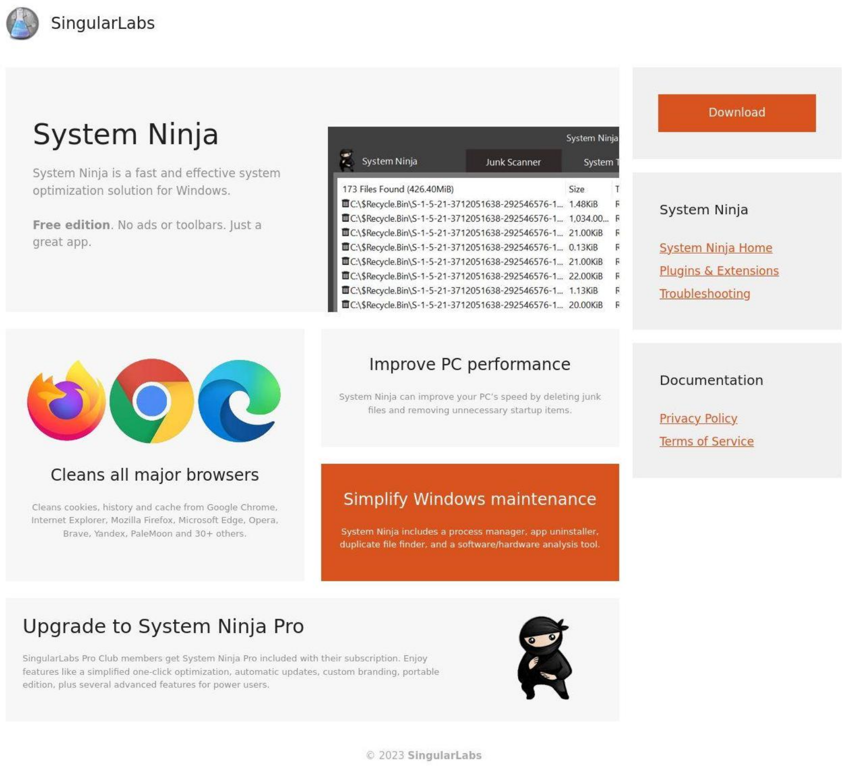


ChatGPT 4 Beta

Our revolutionary new program has taken communication to the next level by integrating cutting-edge technology to allow users to communicate with a chatGPT. This powerful technology is able to understand and interpret human language and respond in a way that mimics natural conversation. Whether you're looking for a quick answer to a question, or want to have a more in-depth conversation, our program is here to provide you with an unmatched level of communication.

Windows 10 - 11 · English
By clicking the "Try it now" button, you accepted all of the Terms and Conditions.

singularlabs.org
(as of January 30, 2023)



SingularLabs

System Ninja

System Ninja is a fast and effective system optimization solution for Windows.

Free edition. No ads or toolbars. Just a great app.

```
                                                        System Ninja
   System Ninja                         Junk Scanner    System T
173 Files Found (426.40MiB)                         Size       T
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  1.48KiB    F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  1,034.00...F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  21.00KiB   F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  0.13KiB    F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  21.00KiB   F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  22.00KiB   F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  1.13KiB    F
C:\$Recycle.Bin\S-1-5-21-3712051638-292546576-1...  20.00KiB   F
```

System Ninja

System Ninja Home
Plugins & Extensions
Troubleshooting

Cleans all major browsers

Cleans cookies, history and cache from Google Chrome, Internet Explorer, Mozilla Firefox, Microsoft Edge, Opera, Brave, Yandex, PaleMoon and 30+ others.

Improve PC performance

System Ninja can improve your PC's speed by deleting junk files and removing unnecessary startup items.

Simplify Windows maintenance

System Ninja includes a process manager, app uninstaller, duplicate file finder, and a software/hardware analysis tool.

Documentation

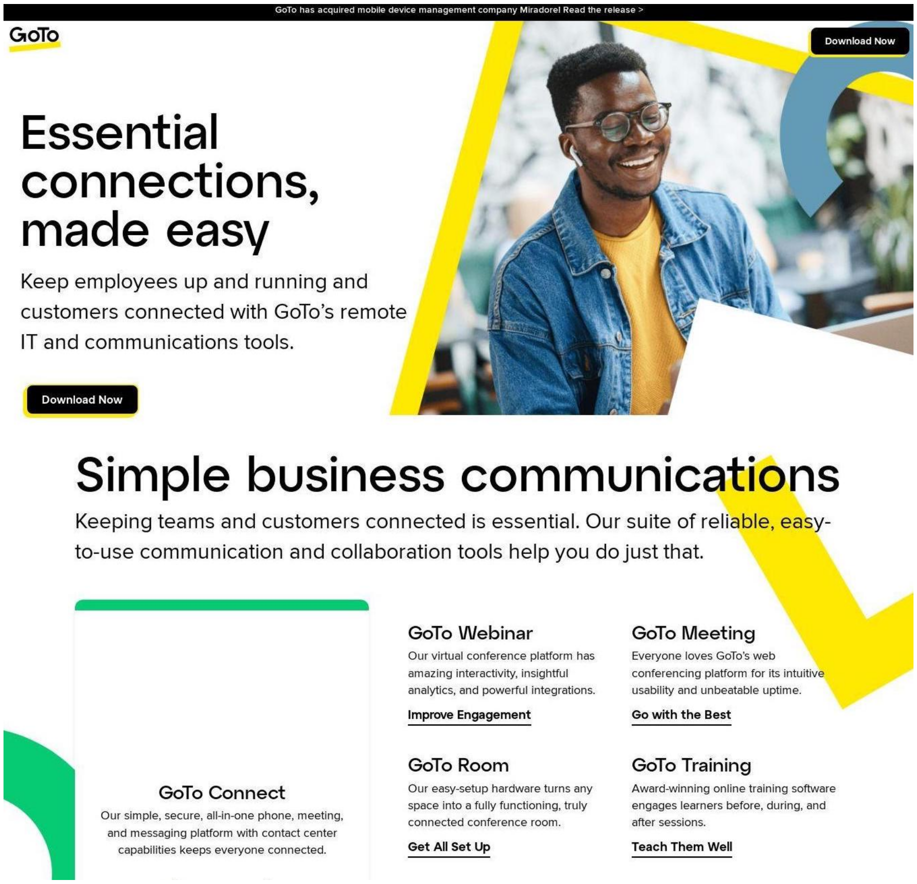
Privacy Policy
Terms of Service

Upgrade to System Ninja Pro

SingularLabs Pro Club members get System Ninja Pro included with their subscription. Enjoy features like a simplified one-click optimization, automatic updates, custom branding, portable edition, plus several advanced features for power users.

© 2023 **SingularLabs**

gotomeet.us
(as of December 14, 2022)



GoTo has acquired mobile device management company Miradore! Read the release >

Essential connections, made easy

Keep employees up and running and customers connected with GoTo's remote IT and communications tools.

Simple business communications

Keeping teams and customers connected is essential. Our suite of reliable, easy-to-use communication and collaboration tools help you do just that.

GoTo Connect

Our simple, secure, all-in-one phone, meeting, and messaging platform with contact center capabilities keeps everyone connected.

GoTo Webinar

Our virtual conference platform has amazing interactivity, insightful analytics, and powerful integrations.

Improve Engagement

GoTo Meeting

Everyone loves GoTo's web conferencing platform for its intuitive usability and unbeatable uptime.

Go with the Best

GoTo Room

Our easy-setup hardware turns any space into a fully functioning, truly connected conference room.

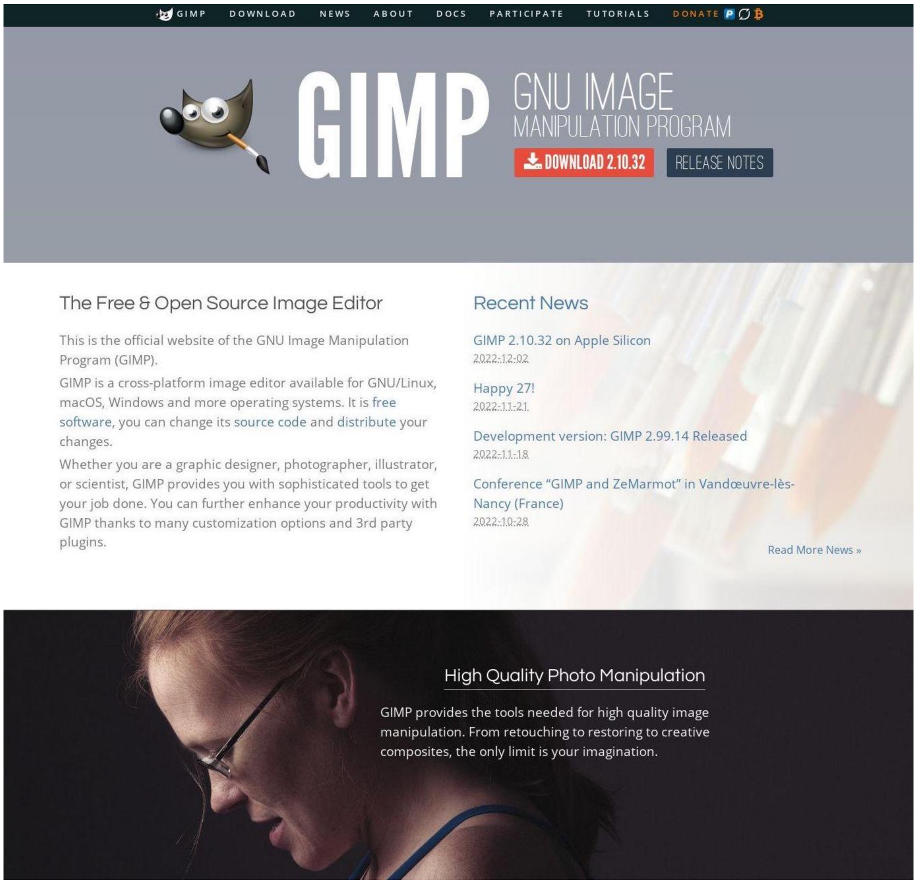
Get All Set Up

GoTo Training

Award-winning online training software engages learners before, during, and after sessions.

Teach Them Well

gllmp.com
(as of December 8, 2022)



The Free & Open Source Image Editor

This is the official website of the GNU Image Manipulation Program (GIMP).

GIMP is a cross-platform image editor available for GNU/Linux, macOS, Windows and more operating systems. It is free software, you can change its source code and distribute your changes.

Whether you are a graphic designer, photographer, illustrator, or scientist, GIMP provides you with sophisticated tools to get your job done. You can further enhance your productivity with GIMP thanks to many customization options and 3rd party plugins.

Recent News

GIMP 2.10.32 on Apple Silicon
2022-12-02

Happy 27!
2022-11-21

Development version: GIMP 2.99.14 Released
2022-11-18

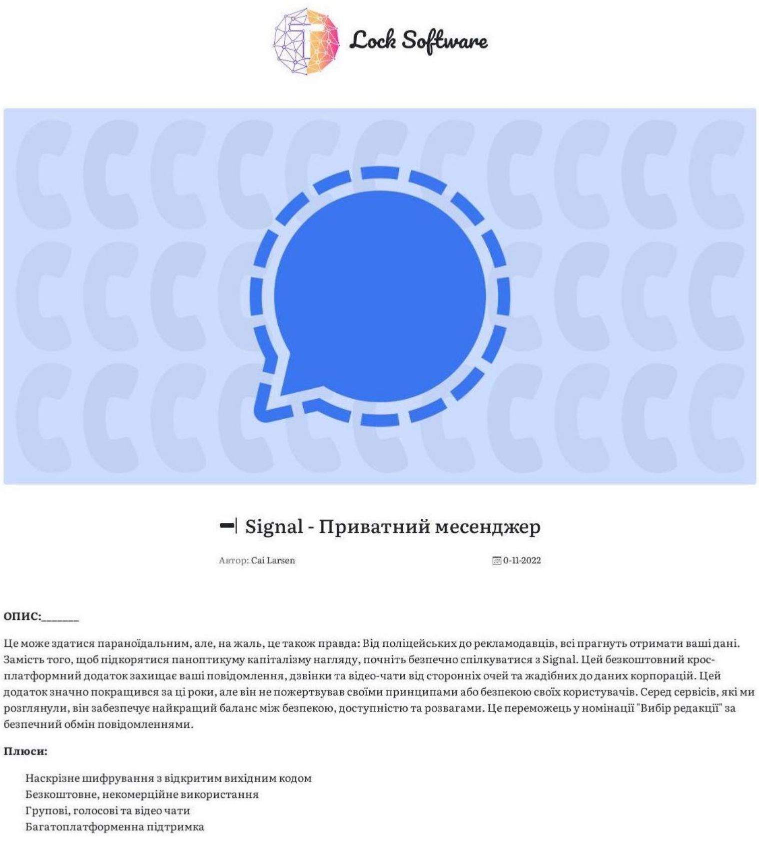
Conference “GIMP and ZeMarmot” in Vandœuvre-lès-Nancy (France)
2022-10-28

Read More News »

High Quality Photo Manipulation

GIMP provides the tools needed for high quality image manipulation. From retouching to restoring to creative composites, the only limit is your imagination.

Info-messengers.com
(as of November 3, 2022)



━| Signal - Приватний месенджер

Автор: Cai Larsen

0-11-2022

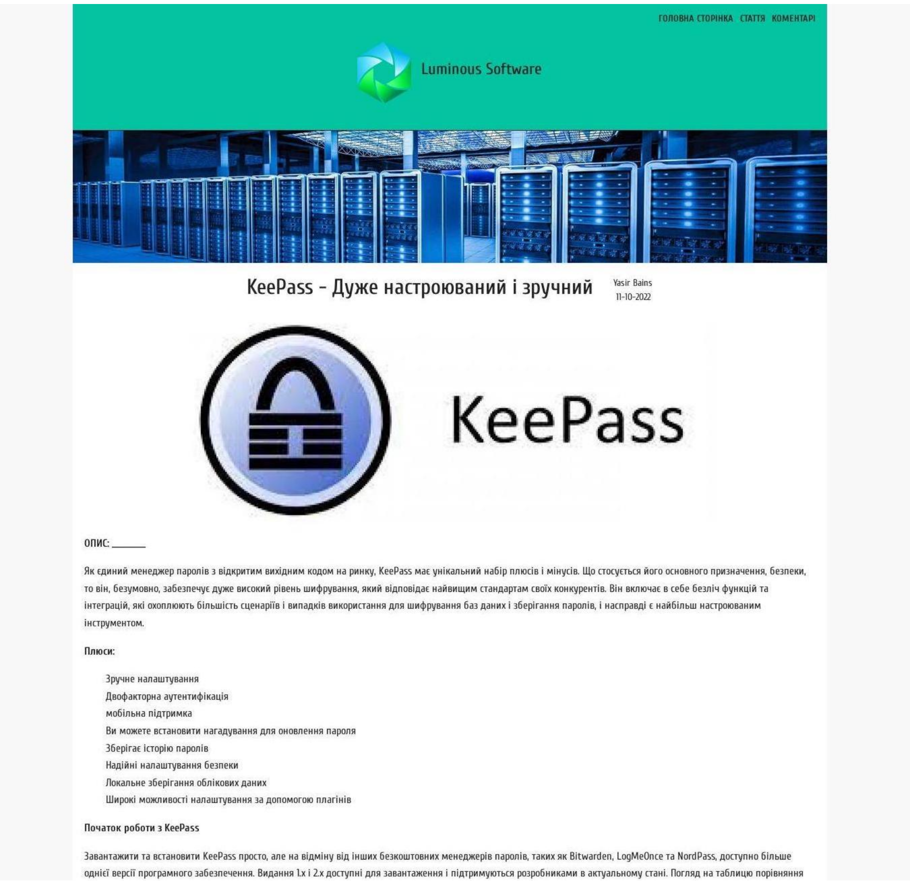
ОПИС:______

Це може здатися параноїдальним, але, на жаль, це також правда: Від поліцейських до рекламодавців, всі прагнуть отримати ваші дані. Замість того, щоб підкорятися паноптикуму капіталізму нагляду, почніть безпечно спілкуватися з Signal. Цей безкоштовний крос-платформний додаток захищає ваші повідомлення, дзвінки та відео-чати від сторонніх очей та жадібних до даних корпорацій. Цей додаток значно покращився за ці роки, але він не пожертвував своїми принципами або безпекою своїх користувачів. Серед сервісів, які ми розглянули, він забезпечує найкращий баланс між безпекою, доступністю та розвагами. Це переможець у номінації "Вибір редакції" за безпечний обмін повідомленнями.

Плюси:

Наскрізне шифрування з відкритим вихідним кодом
Безкоштовне, некомерційне використання
Групові, голосові та відео чати
Багатоплатформенна підтримка

pass-shield.com
(as of October 15, 2022)



KeePass - Дуже настроюваний і зручний

Yasir Bains
11-10-2022

ОПИС: _______

Як єдиний менеджер паролів з відкритим вихідним кодом на ринку, KeePass має унікальний набір плюсів і мінусів. Що стосується його основного призначення, безпеки, то він, безумовно, забезпечує дуже високий рівень шифрування, який відповідає найвищим стандартам своїх конкурентів. Він включає в себе безліч функцій та інтеграцій, які охоплюють більшість сценаріїв і випадків використання для шифрування баз даних і зберігання паролів, і насправді є найбільш настроюваним інструментом.

Плюси:

Зручне налаштування
Двофакторна аутентифікація
мобільна підтримка
Ви можете встановити нагадування для оновлення пароля
Зберігає історію паролів
Надійні налаштування безпеки
Локальне зберігання облікових даних
Широкі можливості налаштування за допомогою плагінів

Початок роботи з KeePass

Завантажити та встановити KeePass просто, але на відміну від інших безкоштовних менеджерів паролів, таких як Bitwarden, LogMeOnce та NordPass, доступно більше однієї версії програмного забезпечення. Видання 1.x і 2.x доступні для завантаження і підтримуються розробниками в актуальному стані. Погляд на таблицю порівняння

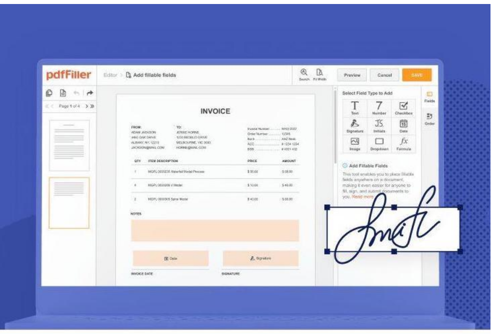
pdffreader.com
(as of October 12, 2022)

PDF Editor для Windows

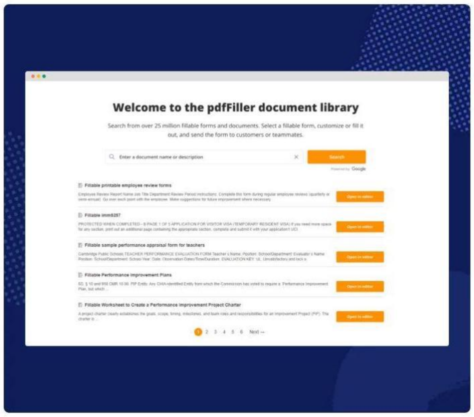
PDFFILLER ДЛЯ WINDOWS BETA

Потужний редактор PDF для вашого ПК

Завантажити



Що ви отримуєте з pdfFiller для Windows beta



Welcome to the pdfFiller document library

Search from over 25 million fillable forms and documents. Select a fillable form, customize or fill it out, and send the form to customers or teammates.

Fillable printable employee review forms

Employee Review Report Name Job Title Department Review Period Instructions: Complete this form during regular employee reviews (quarterly or semi-annual). Go over each point with the employee. Make suggestions for future improvement where necessary.

Fillable imm5257

PROTECTED WHEN COMPLETED - B PAGE 1 OF 5 APPLICATION FOR VISITOR VISA (TEMPORARY RESIDENT VISA) If you need more space for any section, print out an additional page containing the appropriate section, complete and submit it with your application1 UCI

Fillable sample performance appraisal form for teachers

Cambridge Public Schools TEACHER PERFORMANCE EVALUATION FORM Teacher's Name: Position: School/Department: Evaluator's Name Position: School/Department: School Year: Date: Observation Dates/Time/Duration: EVALUATION KEY: UL: Unsatisfactory and lack a

Fillable Performance Improvement Plans

SD, § 10 and 958 CMR 10.00. PIP Entity. Any CHIA-identified Entity from which the Commission has voted to require a Performance Improvement Plan, but which ...

Fillable Worksheet to Create a Performance Improvement Project Charter

A project charter clearly establishes the goals, scope, timing, milestones, and team roles and responsibilities for an Improvement Project (PIP). The charter is ...

Потужний PDF-редактор, який дозволяє працювати з документами вітерець

Змініть текст, виділіть або затемніть вміст, додайте підписи, перетворювати документи на шаблони тощо.

Заповнювані PDF-форми для збору даних і підписів онлайн

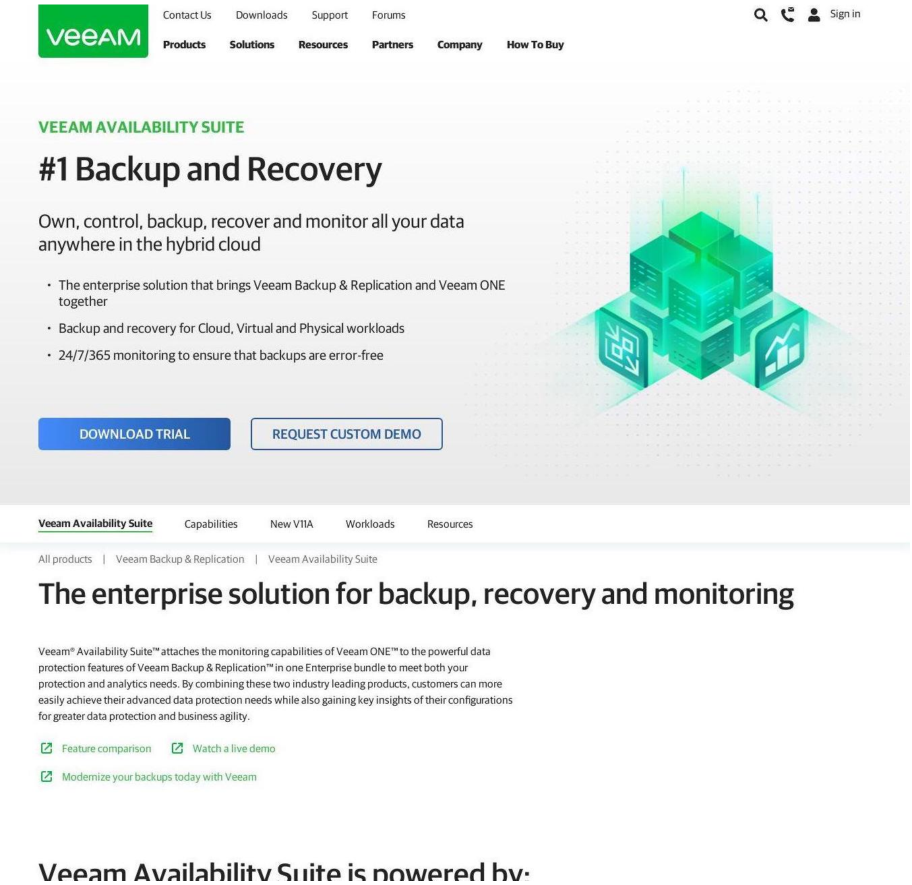
Необмежене та безпечне зберігання документів у хмарі

Бібліотека з 25 мільйонами безкоштовних документів, готових для завантаження

Керуйте документами на ПК як професіонал

Бета-версія pdfFiller для Windows була розроблена з урахуванням продуктивності. Він надає вам усі інструменти, необхідні для роботи з документами ефективно. Встановіть програму для комп'ютера та почніть редагувати, підписувати, та безпечне зберігання документів у хмарі.

veeame.com
(as of September, 9
2022)



VEEAM AVAILABILITY SUITE

#1 Backup and Recovery

Own, control, backup, recover and monitor all your data anywhere in the hybrid cloud

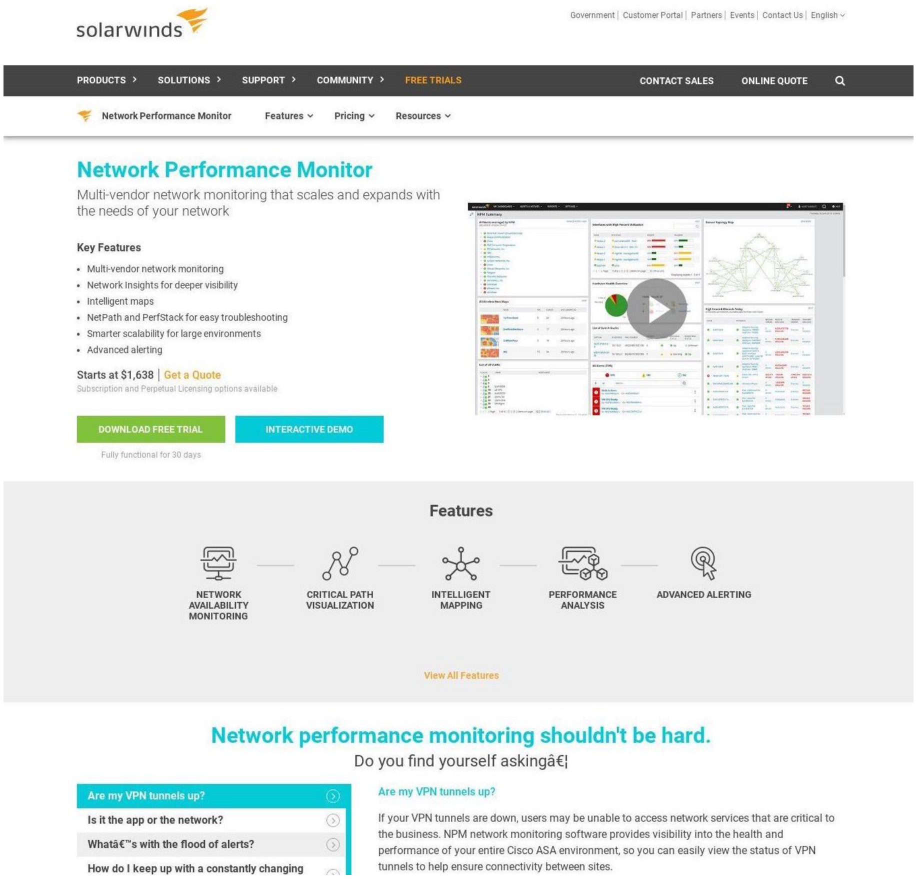
- The enterprise solution that brings Veeam Backup & Replication and Veeam ONE together
- Backup and recovery for Cloud, Virtual and Physical workloads
- 24/7/365 monitoring to ensure that backups are error-free

The enterprise solution for backup, recovery and monitoring

Veeam® Availability Suite™ attaches the monitoring capabilities of Veeam ONE™ to the powerful data protection features of Veeam Backup & Replication™ in one Enterprise bundle to meet both your protection and analytics needs. By combining these two industry leading products, customers can more easily achieve their advanced data protection needs while also gaining key insights of their configurations for greater data protection and business agility.

Veeam Availability Suite is powered by:

npm-solar.com
(as of July 31, 2022)



Network Performance Monitor

Multi-vendor network monitoring that scales and expands with the needs of your network

Key Features

- Multi-vendor network monitoring
- Network Insights for deeper visibility
- Intelligent maps
- NetPath and PerfStack for easy troubleshooting
- Smarter scalability for large environments
- Advanced alerting

Starts at $1,638 | Get a Quote

Subscription and Perpetual Licensing options available

Features

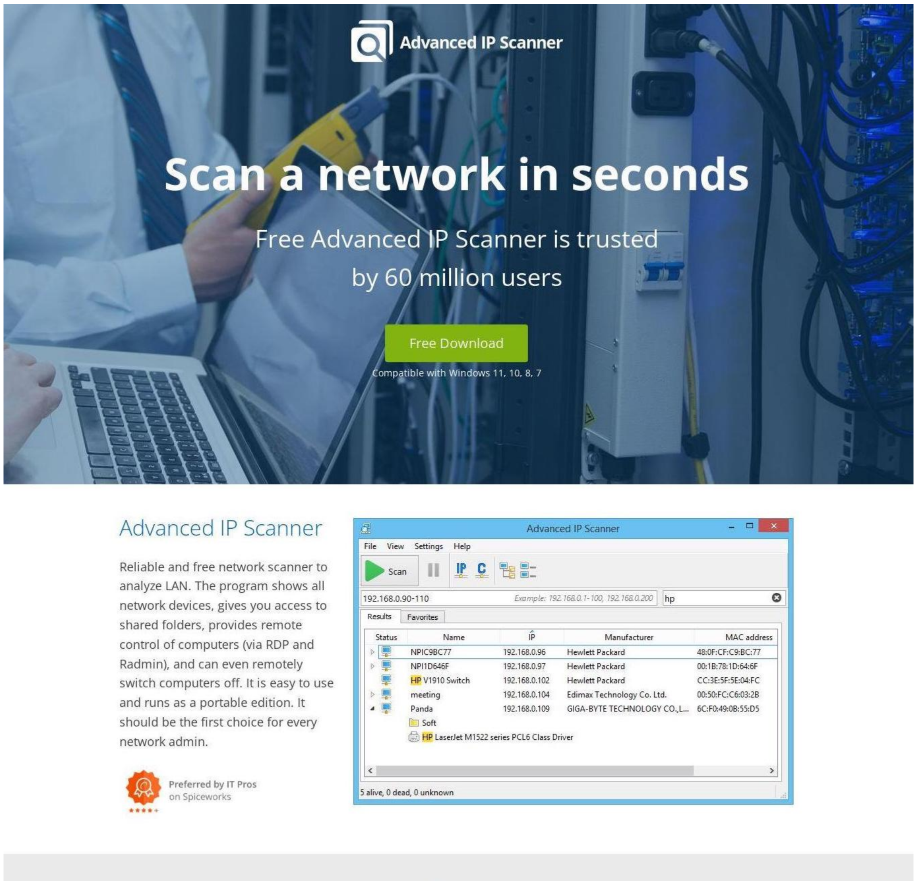
Network performance monitoring shouldn't be hard.

Do you find yourself askingâ€¦

Are my VPN tunnels up?
Is it the app or the network?
Whatâ€™s with the flood of alerts?
How do I keep up with a constantly changing

Are my VPN tunnels up?

If your VPN tunnels are down, users may be unable to access network services that are critical to the business. NPM network monitoring software provides visibility into the health and performance of your entire Cisco ASA environment, so you can easily view the status of VPN tunnels to help ensure connectivity between sites.

advanced-ip-scanners.com (as of July 20, 2022)	 Scan a network in seconds Free Advanced IP Scanner is trusted by 60 million users Compatible with Windows 11, 10, 8, 7 Advanced IP Scanner Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first choice for every network admin. Preferred by IT Pros on Spiceworks

```
192.168.0.90-110          Example: 192.168.0.1-100, 192.168.0.200     hp
Results   Favorites
Status  Name                 IP              Manufacturer                   MAC address
        NPIC9BC77            192.168.0.96    Hewlett Packard                48:0F:CF:C9:BC:77
        NPI1D646F            192.168.0.97    Hewlett Packard                00:1B:78:1D:64:6F
        HP V1910 Switch      192.168.0.102   Hewlett Packard                CC:3E:5F:5E:04:FC
        meeting              192.168.0.104   Edimax Technology Co. Ltd.     00:50:FC:C6:03:2B
        Panda                192.168.0.109   GIGA-BYTE TECHNOLOGY CO.,L...  6C:F0:49:0B:55:D5
          Soft
          HP LaserJet M1522 series PCL6 Class Driver
5 alive, 0 dead, 0 unknown
```

Table 1. RomCom lure sites
Image credit: DomainTools

As reported by the Ukrainian Computer Emergency Response Team (CERT-UA) in the fall of 2022, RomCom was used in specific campaigns against Ukrainian targets, including the Ukrainian government and the Ukrainian military. Trend Micro's telemetry confirms this targeting, and, as shown in a selection of the numerous RomCom campaigns over time (Table 1), it is immediately clear that RomCom already had Ukrainian-language social engineering lures back in October and November 2022.

We count a few dozen lure websites that have been set up since July 2022. RomCom shows a mix in their targeting methodologies, mixing typical cybercriminal TTPs with TTPs that are more common for APT actors. For example, RomCom used spear phishing against a member of a European parliament in March 2022, but targeted a European defense company in October 2022 with a Google Ads advertisement that led to an intermediary landing site that would redirect to a RomCom lure site. That intermediary landing site used the domain name "*kagomadb[.]com*," which was later used for Qakbot and Gozi payloads in December 2022.

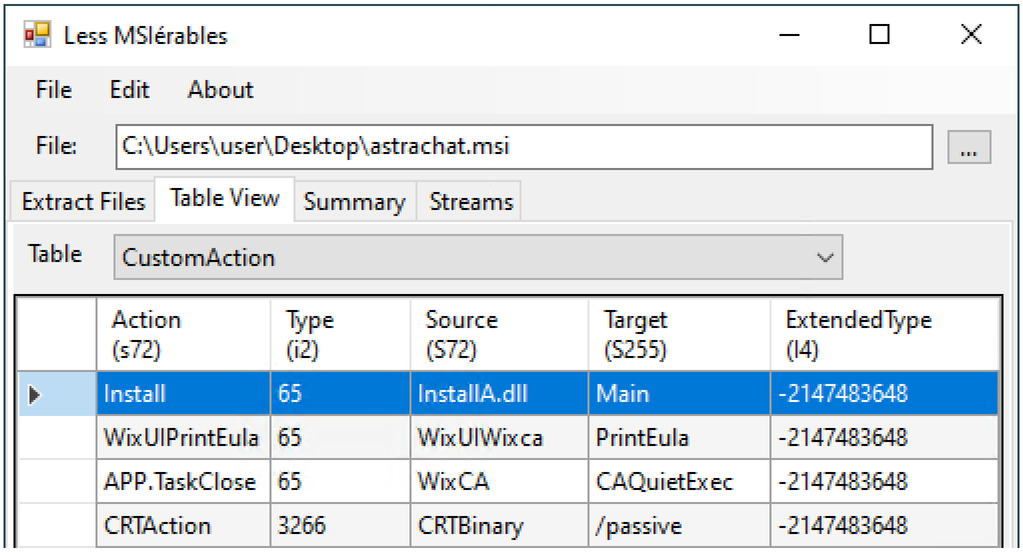
Among the targets we have seen based on Trend Micro's telemetry were a water utility company, entities in the financial and energy sectors, and an IT company in Ukraine. Outside Ukraine, other targets included a local government agency that supports Ukrainian refugees, a defense company in Europe, a high-profile European politician, several IT service providers in Europe and the US, a bank in South America, and a couple of targets located in Asia. Combined with the targets that were published by CERT-UA and Google, a clear picture emerges of the RomCom backdoor's targets: select Ukrainian targets and allies of Ukraine.

RomCom 3.0: The AstraChat Campaign

In this section, we will analyze one of the RomCom backdoor samples that was used in February 2023 against targets in Eastern Europe. Previous RomCom versions analyzed by Palo Alto's Unit 42 use a modular architecture and support up to 20 different commands. Since then, the malware evolved significantly in terms of the number of supported commands, but its modular architecture remains almost unchanged. The threat actor behind RomCom 3.0 also makes use of different techniques to drop and execute the malware. This analysis is based on a campaign that embedded RomCom 3.0 in an AstraChat instant messaging software installation package.

Dropper

The file *astrachat.msi* is a Microsoft Installer (MSI) archive. Despite installing files related to legitimate AstraChat software, it unpacks a malicious *InstallA.dll* file and calls its *Main()* function (Figure 1).



File: C:\Users\user\Desktop\astrachat.msi

Table CustomAction

Action (s72)	Type (i2)	Source (S72)	Target (S255)	ExtendedType (I4)
Install	65	InstallA.dll	Main	-2147483648
WixUIPrintEula	65	WixUIWixca	PrintEula	-2147483648
APP.TaskClose	65	WixCA	CAQuietExec	-2147483648
CRTAction	3266	CRTBinary	/passive	-2147483648

Figure 1. CustomAction table from a RomCom MSI dropper

The *InstallA.dll* file extracts three Dynamic Link Libraries (DLLs) files under the *%PUBLIC%\Libraries* folder:

- *prxyms<number>.dll*

- *winipfile<number>.dll0*
- *netid<number>.dll0*

The number in these DLL files is an integer number based on the Machine GUID read from Windows Registry at *HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid*.

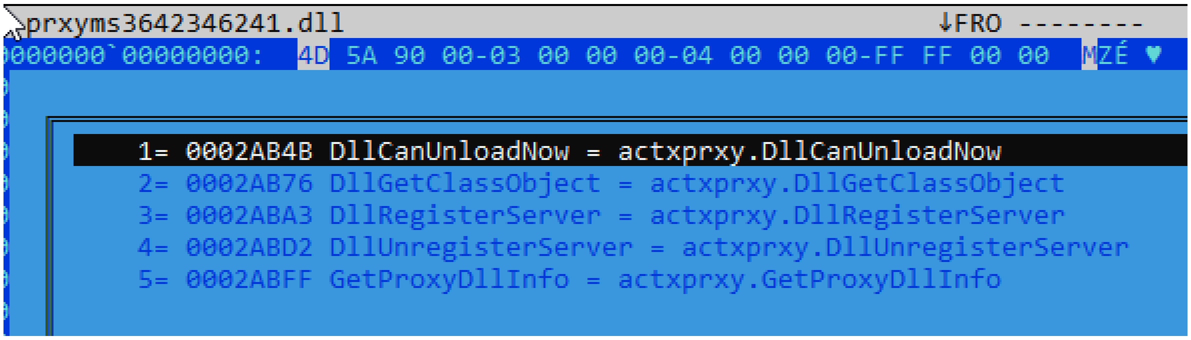
Persistence

For persistence, RomCom uses COM hijacking, hence its name. *InstallA.dll* writes the following registry value in Windows Registry:

[HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6}\InProcServer32]
@="%PUBLIC%\\Libraries\\prxyms<number>.dll"

This overwrites the same key under the *HKEY_LOCAL_MACHINE* hive, causing processes that request this Class ID (CLSID) to load the RomCom loader DLL at *%PUBLIC%\Libraries\prxyms<number>.dll*. One such process is *explorer.exe*, which is restarted by RomCom dropper, so the loader DLL is called.

The RomCom loader also redirects calls to its exported functions to the legit *actxprxy.dll* by making use of forwarded exports (Figure 2).



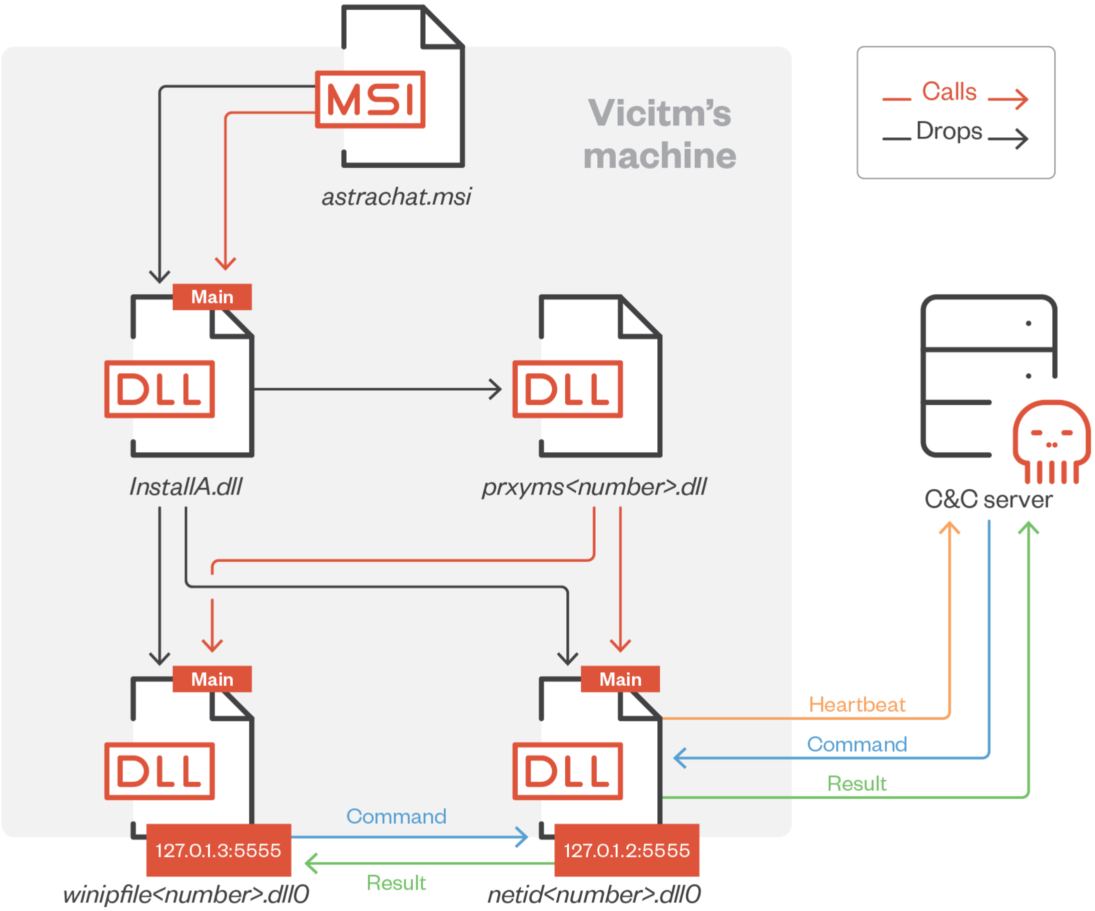
```
prxyms3642346241.dll                                        ↓FRO --------
000000`00000000:   4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00   MZÉ ♥

      1= 0002AB4B DllCanUnloadNow = actxprxy.DllCanUnloadNow
      2= 0002AB76 DllGetClassObject = actxprxy.DllGetClassObject
      3= 0002ABA3 DllRegisterServer = actxprxy.DllRegisterServer
      4= 0002ABD2 DllUnregisterServer = actxprxy.DllUnregisterServer
      5= 0002ABFF GetProxyDllInfo = actxprxy.GetProxyDllInfo
```

Figure 2. Forwarded exports from the RomCom 3.0 loader (*prxyms<number>.dll*)

However, before a call is forwarded, the malicious code at the DLL entry point of RomCom loader runs. This code uses *rundll32.exe* to execute the exported *Main()* function from both *winipfile<number>.dll0* and *netid<number>.dll0*.

Architecture

RomCom 3.0 is divided into three components: a loader, a network component that interacts with the command-and-control (C&C) server, and a worker component that performs the actions on the victim's machine. The network component is handled by *netid<number>.dll0*, which is responsible for receiving commands from the C&C server and sending back their results. When this component receives a command, the command is sent through a localhost socket to *winipfile<number>.dll0*, which handles the worker component, as shown in Figure 3. If initial loopback addresses or ports are in use, both components try to find other available combinations.



©2023 TREND MICRO

Figure 3. Overall RomCom 3.0 architecture

Bot Commands

RomCom 3.0 commands are received as responses to HTTP POST requests made by the malware network component.

4-byte ID	1-byte command	Variable length additional command data
59 09 00 00	05	AC 03 00 00

©2023 TREND MICRO

Figure 4. RomCom 3.0 command structure

Figure 4 shows an example of command 5 – a command to download a file to the victim's machine – being received. The ID used for communication is *0x950*, and command *0x05* is received with additional data. In this case, the additional data tells the malware running on the infected machine that the downloaded file should occupy 939 (0x3ac – 1) 4KB blocks. The file itself is downloaded in a separate response, so in this instance, the final file size on the victim's side will be 3,846,144 bytes. As an evasion technique, null bytes are appended to the file to achieve this result. The contents of the additional data field may vary according to the command.

In RomCom 3.0, we could enumerate 42 valid commands, as shown in Table 2. This is a high number of commands for a regular backdoor, but a few commands are simply variations of others.

Command	**Purpose (from the victim's perspective)**
1	Send information about connected drives
2	Send a list of file names under a specified directory
3	Start *cmd.exe* to run an existing program
4	Upload a specified file to the C&C server
5	Download a file to the victim's machine
6	Delete a specified file in the victim's machine
7	Delete a specified directory in the victim's machine
8	Spawn a given process with PID spoofing (the PID is also given as part of the command data)
12	Call *startWorker()* from *%PUBLIC%\Libraries\PhotoDirector.dll*, then send *%PUBLIC%\Libraries\PhotoDirector.zip* to the C&C server and delete it
13	Call *startWorker()* from *%PUBLIC%\Libraries\PhotoDirector.dll* and write screen information to *%PUBLIC%\Libraries\update.conf*
14	Upload *%PUBLIC%\Libraries\PhotoDirector.zip* to the C&C server and delete it
15	Send a list of running process with its PIDs
16	Send a list of installed software
17	Delete the worker component (*winipfile<number>.dll0*)
18	Download a file and save it to *%PUBLIC%\Libraries\PhotoDirector.dll*

19	Download a file, save it to *%PUBLIC%\Libraries\BrowserData\procsys.dll*, and call its *stub()* exported function
20	Download a ZIP archive likely containing 3proxy and plink (see command 21)
21	Use 3proxy and plink to set up a proxy via SSH. The IP address, password, local, and remote ports are received as command parameters. SSH server username is fixed as “john.”
22	Kill the *3proxy.exe* and *plink.exe* processes
23	Download a file and save it to *%PUBLIC%\Libraries\upd-fil<number>.dll0* to update the worker
24	Send the contents of *%PUBLIC%\Libraries\BrowserData\Result*
25	Duplicate the worker
26	Send the Windows version
29	Download freeSSHd from the C&C server
30	Run freeSSHd and use plink to create a reverse connection with 51.195.49.215 using “john” as the username and “eK6czNHWCT569L1xK9ZH” as the password
31	Kill the freeSSHd process
32	Send .txt, .rtf, .xls, .xlsx, .ods, .cmd, .pdf, .vbs, .ps1, .one, .kdb, .kdb, .doc, .doc, .odt, .eml, .msg, and .email files in Downloads, Documents, and Desktop folders under *%USERPROFILE%*
34	Run AnyDesk on the victim’s machine on a hidden window and send the AnyDesk ID to the C&C server
35	Kill the AnyDesk process and delete its executable
36	Download the AnyDesk executable and save it to *%PUBLIC%\Libraries\dsk.exe*
38	Download a file and save it to *%PUBLIC%\Libraries\wallet.exe*
39	Download a file and save it to *%PUBLIC%\Libraries\7z.dll*
40	Download a file and save it to *%PUBLIC%\Libraries\7z.exe*
41	Send the contents of *%PUBLIC%\Libraries\tempFolder* compressed with 7-Zip
42	Download a file and save it to *%PUBLIC%\Libraries\7za.exe*

43	Use *%PUBLIC%\Libraries\7za.exe* to compress a given folder to a *fold.zip* archive and send the compressed archive to the C&C server
44	Kill the *PhotoDirector.dll* process
45	Download a file and save it to *%PUBLIC%\Libraries\msg.dll*
46	Call *stW()* function exported by *%PUBLIC%\Libraries\msg.dll*
47	Download a file and save it to *%PUBLIC%\Libraries\FileInfo.dll*
48	Call *fSt()* function exported by *%PUBLIC%\Libraries\FileInfo.dll*
49	Update the network component

Table 2. RomCom 3.0 commands

Additional Malware

Based on messages sent back to the C&C server and how the commands use these files, we can infer the purpose of a few additional components:

- ***PhotoDirector.dll*** – a program that takes one or more screenshots and compresses them in a *%PUBLIC%\Libraries\PhotoDirector.zip* archive
- ***procsys.dll*** – a stealer known as STEALDEAL to retrieve browser cookies and write them to *%PUBLIC%\Libraries\BrowserData\Result*
- ***wallet.exe*** – a crypto wallet grabber that writes stolen information to *%PUBLIC%\Libraries\tempFolder*
- ***msg.dll*** – an Instant Messaging grabber to steal chat messages
- ***FileInfo.dll*** – a stealer of FTP credentials, or a component to make the victim's machine upload files to an FTP server

Despite these additional pieces of malware, RomCom 3.0 also seems to have commands to download and run legitimate software:

- ***dsk.exe*** – a portable version of AnyDesk software
- ***7z.dll***, ***7z.exe***, and ***7za.exe*** – files related to the 7-Zip program

---

STEALDEAL

The stealer that is downloaded through RomCom's C&C servers is a relatively simple one that steals stored credentials and browsing history from the following browsers:

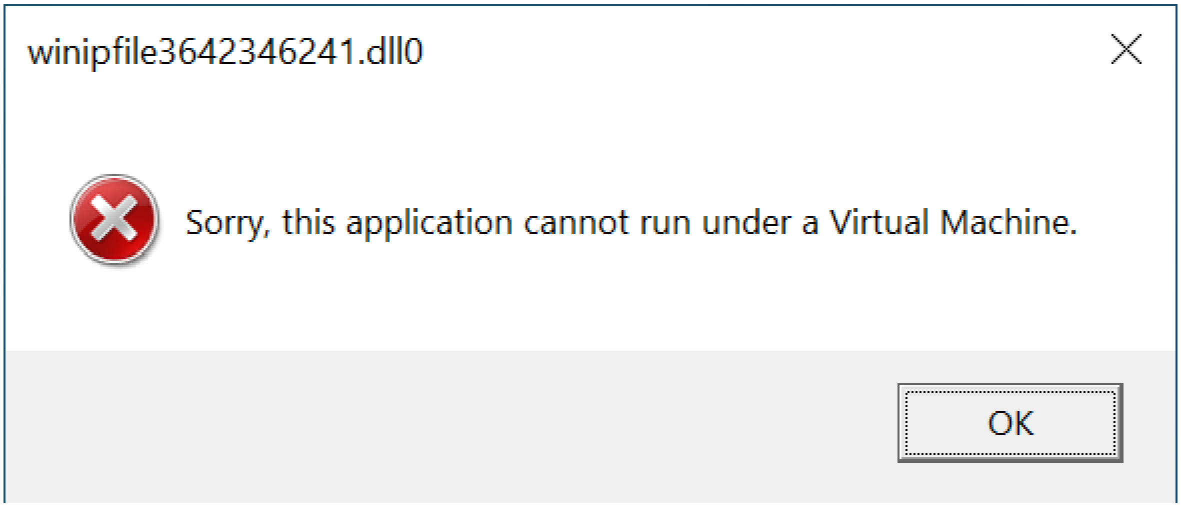
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

- Chromium
- Chrome Beta
- Yandex Browser

The stealer also collects information on installed mail clients. The stolen data is stored locally on the victim’s machine at *%PUBLIC%\Libraries\BrowserData\Result*, and through C&C command 24, this data is exfiltrated through a RomCom C&C server. We detected the stealer as *TrojanSpy.Win64.STEALDEAL*, which is also known as SneakyStealer.

Evasion Techniques

RomCom 3.0 binaries are protected with VMProtect. Some binaries are also signed with valid certificates. Because the actors decided to use VMProtect’s anti-VM feature, any attempt to run it in a virtual machine (VM) without modification or VM hardening will cause the malware to show an error message and exit (Figure 5).


winipfile3642346241.dll0

Sorry, this application cannot run under a Virtual Machine.

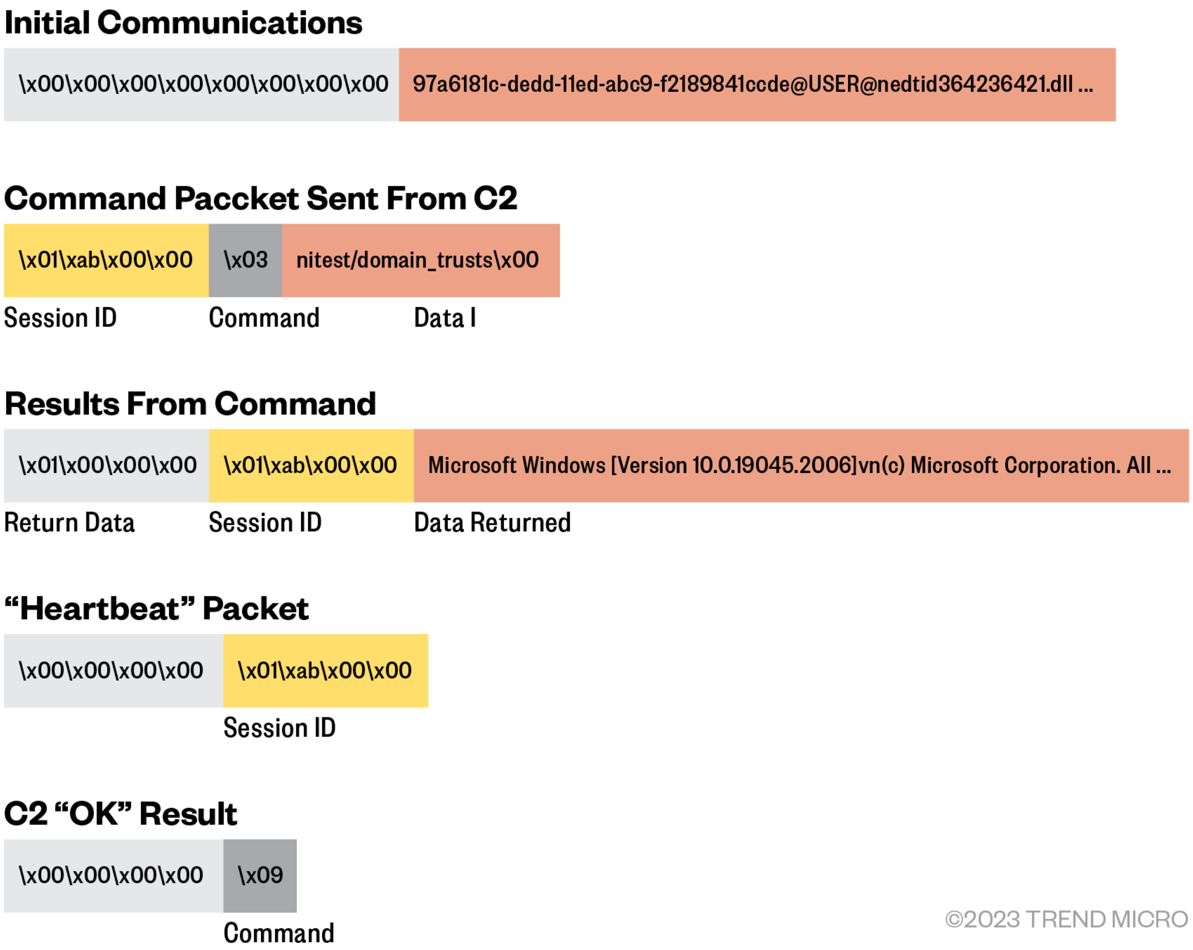
Figure 5. Default VMProtect anti-VM detection in RomCom 3.0 samples

Another interesting technique RomCom uses is the ability to add null bytes appended to the files received from a C&C server. Making the file bigger can be an attempt to avoid sandbox products or security software scanners that impose a file size limit.

In later versions of RomCom, the binary that is hosted on a lure site contains an encrypted payload. To correctly decrypt the payload, it will need to reach out to a web server at the IP address 94.142.138.244 and download the decryption key. We suspect this website is a third-party service that is also being used by other malware, including the Vidar stealer that is also known as StealC. Also, recent RomCom droppers have stopped dropping the worker component. Instead, the network component downloads it from the C&C server.

Packet Structure and Communications Flow

Based on our observations of the communication between victim machines and RomCom C&C servers, we were able to determine what the packet structure of this communication looks like (Figure 6). Initially, the client will reach out to the server with information on the victim's computer, such as its Universally Unique Identifier (UUID), username, and the computer name. The server will then respond with a session ID that is four bytes long, as mentioned previously. This session ID is then incremented by one on the first byte by the C&C server with each command that is sent to the victim machine.



Initial Communications

\x00\x00\x00\x00\x00\x00\x00\x00	97a6181c-dedd-11ed-abc9-f2189841ccde@USER@nedtid364236421.dll ...

Command Paccket Sent From C2

Session ID	Command	Data I
\x01\xab\x00\x00	\x03	nitest/domain_trusts\x00

Results From Command

Return Data	Session ID	Data Returned
\x01\x00\x00\x00	\x01\xab\x00\x00	Microsoft Windows [Version 10.0.19045.2006]vn(c) Microsoft Corporation. All ...

"Heartbeat" Packet

	Session ID
\x00\x00\x00\x00	\x01\xab\x00\x00

C2 "OK" Result

	Command
\x00\x00\x00\x00	\x09

©2023 TREND MICRO

Figure 6. Packet structure of the observed packets

One of the first commands we observed was command 3, which uses *cmd.exe* to run a *Nltest* command with the argument */domain_trusts*. This is done to gather information on any domains that the victim machine may know about. Once the command is finished, it returns the results of the command with the Session ID five bytes in; the first four bytes are unknown at this time, but we observed the first byte will be 0x01 if it is returning data to the server, or 0x00 if it is receiving data from the server. The C&C server then appears to ask for specific information in an automated manner, as the same requests are sent in quick succession (Figure 7). From our analysis, we have determined that the server is asking for the victim machine to:

1. Return *ntlest /domain_trusts* with command 3
2. Download StealDeal to collect certain information
3. Use StealDeal to collect cookies and other information from the victim's machine
4. Collect files from the Desktop, Documents, and Downloads folders using command 32

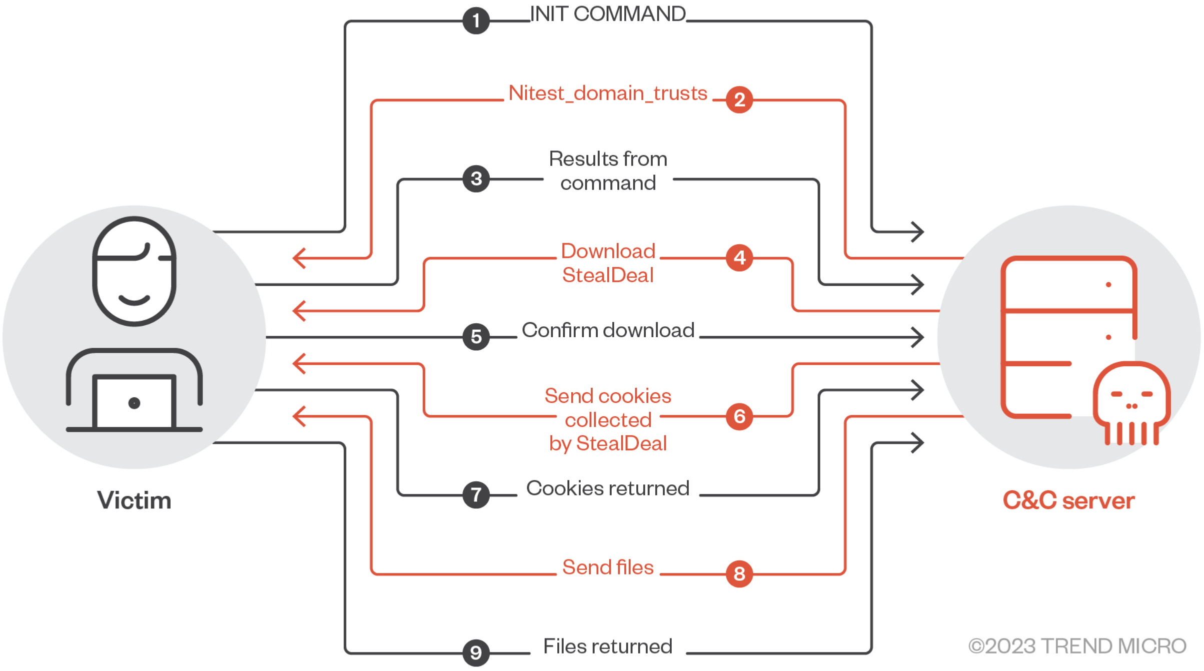
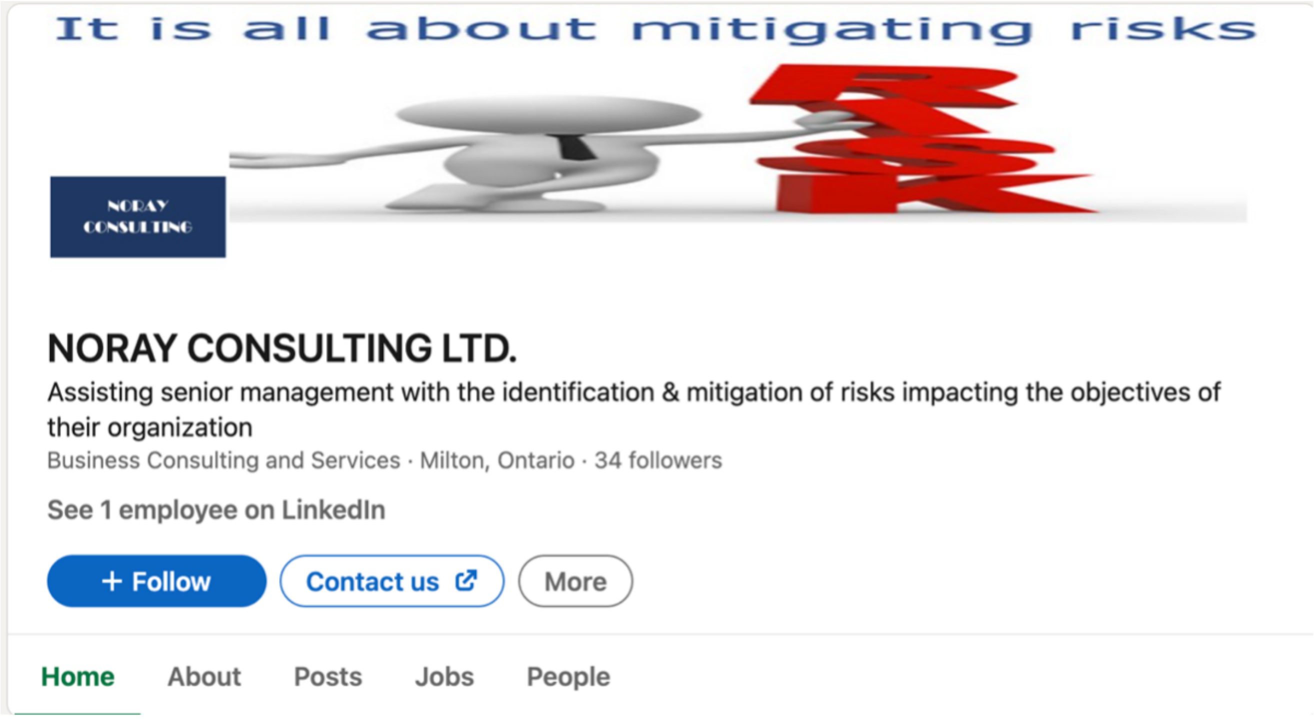


Figure 7. Flow of the communication between the C&C server and victim machine

Use of fake companies and websites

The malware uses certificates to lend credibility to the software that the targeted victims download. On the surface, the companies that are signing these binaries look like legitimate companies that have undergone the process of becoming a signer of these certificates. However, a closer look at these companies' websites reveals several oddities, including non-existent phone numbers, stock photos of executives, office addresses that do not seem to match. This leads us to believe these are either fake companies or legitimate companies that are being abused in order to pass the checks needed to become an authorized signer of binaries.

The RomCom 3.0 sample that was used in the AstraChat campaign was signed by a Canadian company called Noray Consulting Ltd., which has a LinkedIn page (Figure 8), a website, and even a listing in a business registry in Canada (Figure 9).



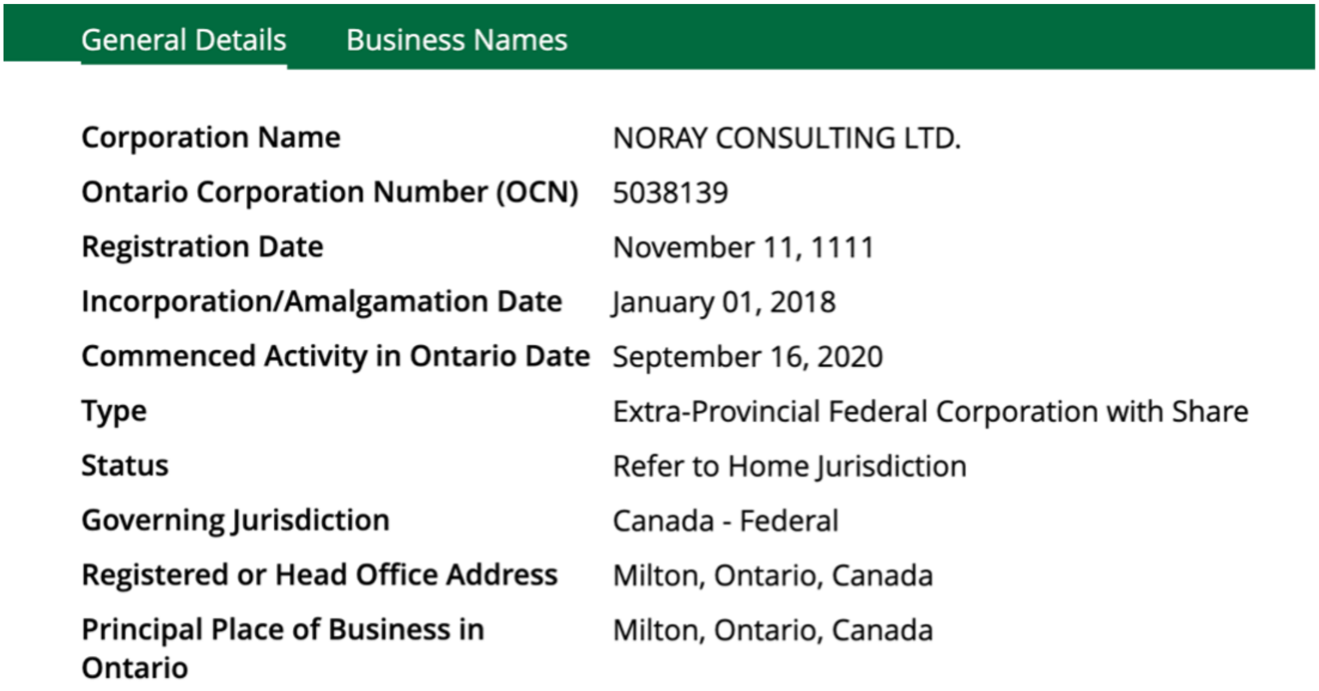
NORAY CONSULTING LTD.

Assisting senior management with the identification & mitigation of risks impacting the objectives of their organization

Business Consulting and Services · Milton, Ontario · 34 followers

See 1 employee on LinkedIn

Figure 8. Screenshot of Noray Consulting's LinkedIn page



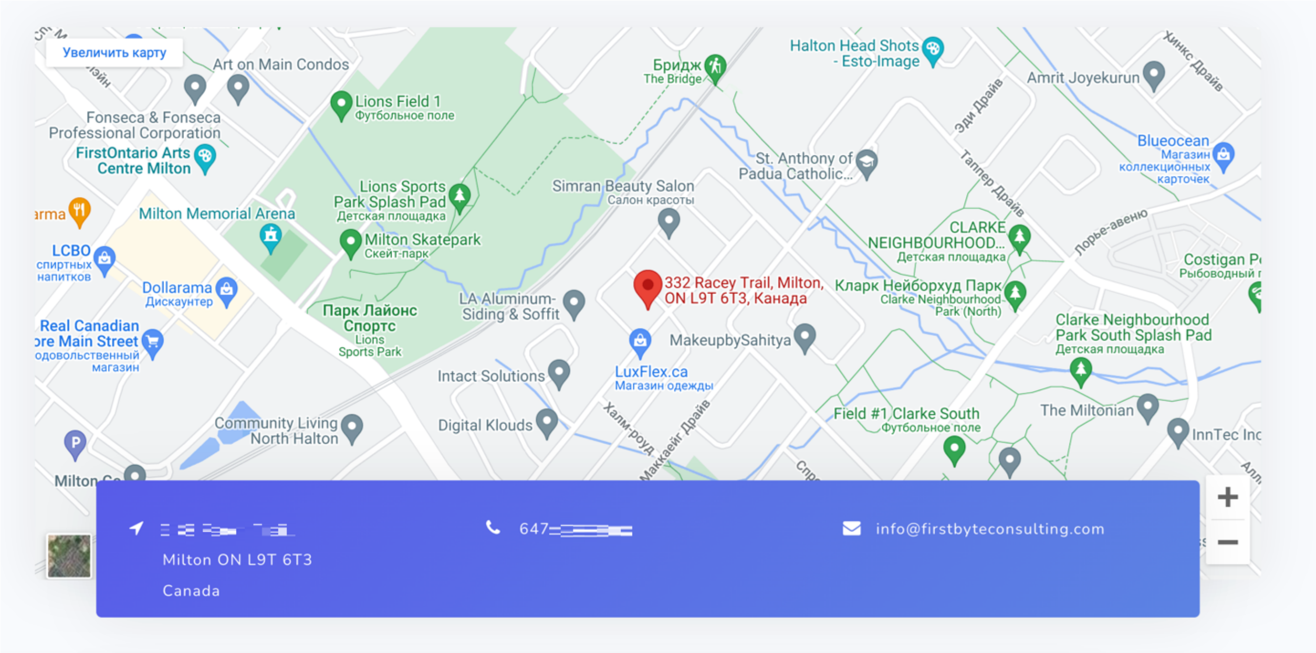
Corporation Name	NORAY CONSULTING LTD.
Ontario Corporation Number (OCN)	5038139
Registration Date	November 11, 1111
Incorporation/Amalgamation Date	January 01, 2018
Commenced Activity in Ontario Date	September 16, 2020
Type	Extra-Provincial Federal Corporation with Share
Status	Refer to Home Jurisdiction
Governing Jurisdiction	Canada - Federal
Registered or Head Office Address	Milton, Ontario, Canada
Principal Place of Business in Ontario	Milton, Ontario, Canada

Figure 9. Ontario business registry search results for Noray Consulting

The company's LinkedIn page goes on to mention that Noray Consulting works on SOX compliance, an annual audit mandated by the Sarbanes-Oxley Act (SOX), as well as other areas of risk control. However, the LinkedIn page also points to a website, *noray[.]ca*, that does not exist.

As the company claims to be based in Ontario according to its LinkedIn page, we looked for any information about it in public records for businesses in Canada. It appears that in 2020, the owners of Noray Consulting. Changed the name of the company to just “Noray.” This new company name is not related to any of the things mentioned in this blog post or, from what we can tell, is doing anything malicious. It appears that the actors are watching out for companies that become inactive, or in a similar status, then will appropriate these companies’ names.

Internet searches for Noray Consulting show that its main website has a non-matching domain name, *firstbyteconsulting[.]com*. The website used to be for a company that specialized in project management. This domain appears to have expired in 2020, but was bought and repurposed to resemble the website from before 2020. What ties this domain to Noray Consulting now is that the address details on the website match that which is found on Noray Consulting’s LinkedIn page: a Canadian company in Milton, Ontario. The contact page has a map that shows the company’s location, but the map is in Russian (Figure 10). This could mean that the person who made this Google map had their primary language set to Russian, which would be unusual for a seemingly Canadian-based company.



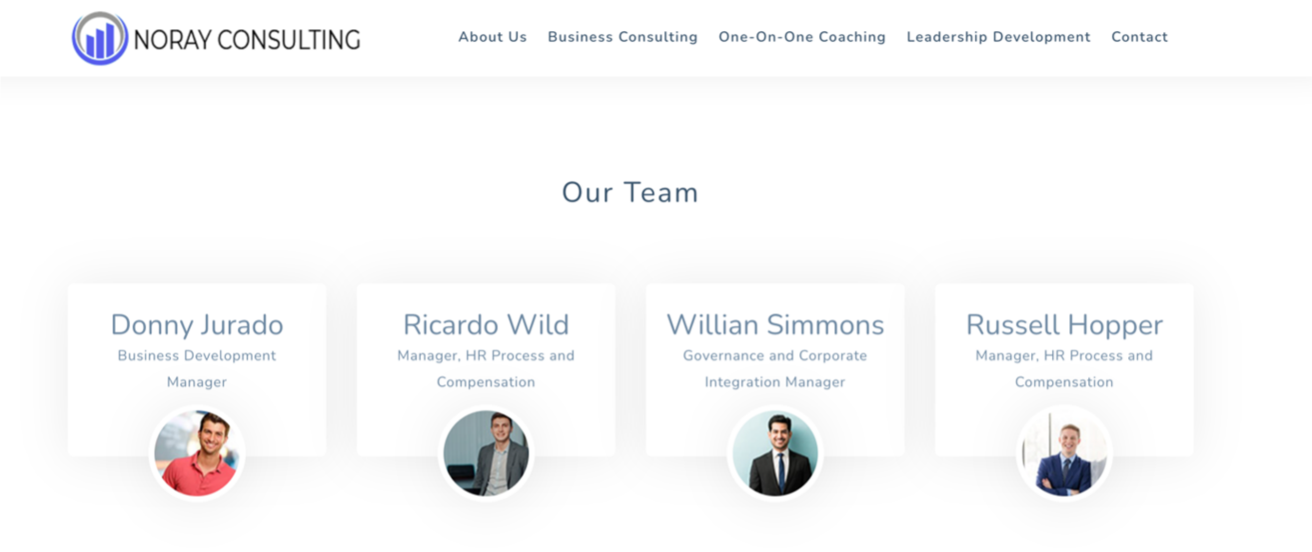
[redacted]
Milton ON L9T 6T3
Canada

647[redacted]

info@firstbyteconsulting.com

Figure 10. Screenshot of the website’s contact page map

We also found that the people mentioned on their website are likely stock images or AI-generated photos of people who are not related in any way to the business, as shown in Figure 11.



Our Team

Donny Jurado
Business Development Manager

Ricardo Wild
Manager, HR Process and Compensation

Willian Simmons
Governance and Corporate Integration Manager

Russell Hopper
Manager, HR Process and Compensation

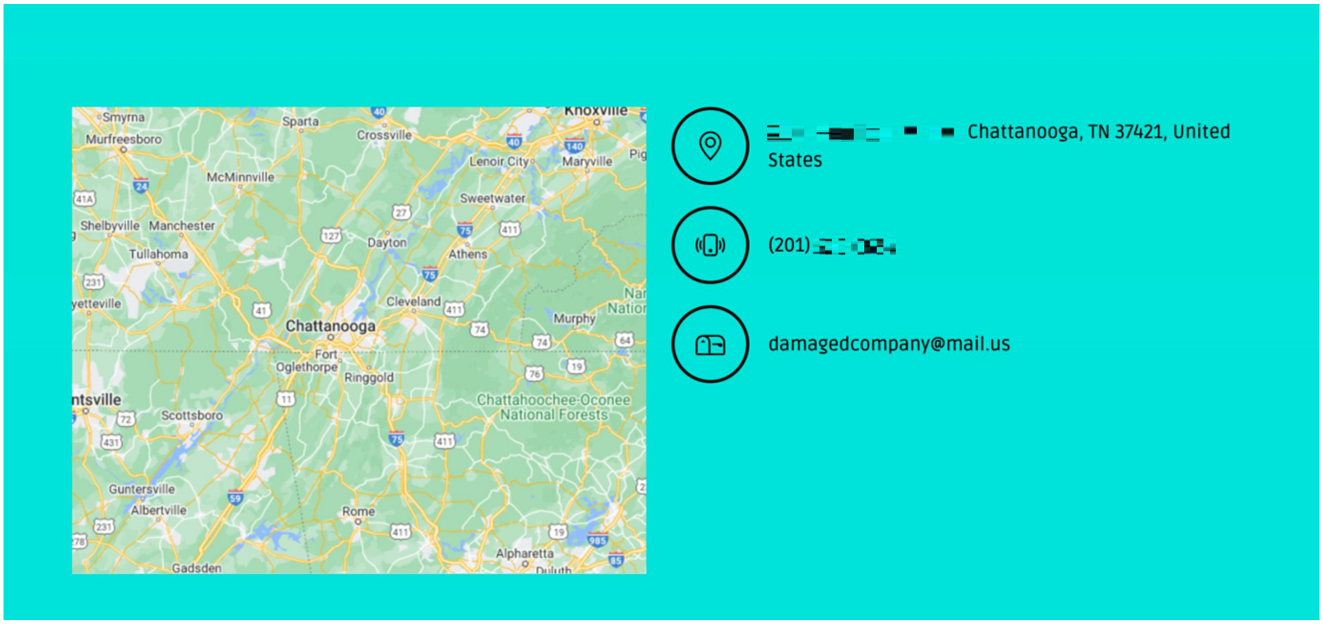
Figure 11. Screenshot of the website's team members page

Further investigation reveals that Figure 11 has a number of red flags:

- None of these people appear to have real personas on the internet
- Reverse image search reveals these are stock photo images used on several sites
- Two members of the team have the same job title of "Manager, HR Process and Compensation"

We have also observed that the text in other parts of Noray Consulting's website has been at least partially copied from other websites. This illustrates that these actors are trying to make the sites believable, offering what seems like realistic services that were lifted from real companies found online.

Void Rabisu has had many lure websites that attempt to convince targets to download trojanized legitimate applications. These lure sites look legitimate at first, but usually have similar oddities on the websites. For example, a site that had a business address of a shopping mall, and the contact phone number of a grocery store.



[redacted] Chattanooga, TN 37421, United States

(201)[redacted]

damagedcompany@mail.us

Figure 12. Screenshot of the contact information of a Void Rabisu lure site

We can link the two Canadian companies that were used to sign RomCom binaries in the AstraChat campaign and a campaign against the Ukrainian armed forces with more than 80 other mostly Canadian companies in total, based on an analysis of internet infrastructure. Among these 80 other mostly Canadian companies, about two dozen companies were used to sign other malware binaries like Emotet, Matanbuchus Loader, BatLoader, another backdoor known as SolarMarker, and coinminers. This makes us believe that Void Rabisu is likely to be using a third-party service that aids in signing binaries with certificates of seemingly legitimate Canadian companies.

Conclusions and Recommendations

The war against Ukraine has made cyber campaigns against Ukraine, Eastern Europe, and NATO countries more visible for two reasons: the number of attacks has increased dramatically, and both the private and public sectors are looking closely at what happens in Ukraine. More information from intelligence agencies is being declassified by Western governments, so privately-owned companies can investigate further for themselves. Another important factor is that many actors who previously had different motivations are becoming more aligned towards the same goal, even when their campaigns do not appear to be part of a coordinated effort.

The line is blurring between cybercrime driven by financial gain and APT attacks motivated by geopolitics, espionage, disruption, and warfare. Since the rise of Ransomware-as-a-Service (RaaS), cybercriminals are now using advanced tactics and targeted attacks that were previously thought to be the domain of APT actors. Inversely, tactics and techniques that were previously used by financially motivated actors are increasingly being used in attacks with geopolitical goals.

Currently, APT actors like Pawn Storm and APT29, cyber mercenaries like Void Balaur, hacktivism groups like Killnet, along with cybercriminals like former Conti affiliates and Void Rabisu, are targeting Ukraine and its allies, but their campaigns do not yet look coordinated. We expect that significant geopolitical events like the current war against Ukraine will accelerate the alignment of the campaigns of threat actors who reside in the same geographic region. This will lead to new challenges for defenders, as attacks can then come from many different angles, and it will be less clear who is the actor responsible for them.

Based on our analysis, we believe the following activity should be monitored in endpoints:

- Downloading and executing MSI packages that contain entries in CustomAction tables referring to DLL exported functions
- Writing access to SOFTWARE\Classes\CLSID\<CSLID> under both *HKEY_CURRENT_USER* (HKCU) and *HKEY_LOCAL_MACHINE* (HKLM), which can be a sign of COM hijacking
- Initiation of localhost sockets by *rundll32.exe*, as RomCom DLLs are loaded by this process — we observed that RomCom listens on the port range 5554-5600 when setting up localhost sockets
- Binary padding with null bytes, a known technique to evade scanners. Although RomCom didn't use this feature in our tests, it is present in command 5. We included a YARA ruleset to look for such files in our GitHub research repository.
- Binary padding with non-zero data, which we observed in one sample when it was dropping another. This alone is not malicious, but it is worth flagging once detected for further investigation.

Endpoint solutions like Trend Micro's Smart Protection Suites and Worry-Free Business Security solutions also offer protection for both users and businesses against threats like RomCom. These solutions come equipped with behavior-monitoring capabilities that enable them to detect malicious files, scripts, and messages. They can also block all related malicious URLs. Additionally, the Trend Micro™ Deep Discovery™ solution includes an email inspection layer that can identify and protect enterprises from malicious attachments and URLs. By leveraging these powerful tools, users and businesses can effectively defend themselves against the damaging effects of RomCom and other similar threats.

Indicators of Compromise

Download the full list of indicators here.

MITRE ATT&CK

ID	Name	Description

T1583.008	Acquire Infrastructure: Malvertising	RomCom uses malvertising to redirect targets to lure websites from which to download fake installer applications
T1566.002	Phishing: Spear Phishing Link	RomCom sent highly targeted spear phishing emails
T1027.002	Obfuscated Files or Information: Software Packing	RomCom uses VMProtect
T1027.001	Obfuscated Files or Information: Binary Padding	RomCom uses binary padding on dropped files to avoid security solutions
T1546.015	Event Triggered Execution: Component Object Model Hijacking	RomCom uses COM hijacking for persistence
T1571	Non-Standard Port	RomCom listens on port ranges 5554 to 5600 for communication between dropped components
T1071.001	Application Layer Protocol: Web Protocols	RomCom uses HTTPS for C&C communications
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	RomCom uses a stealer to gather credentials of several browsers
T1113	Screen Capture	RomCom can capture screenshots of the victim's machine
T1219	Remote Access Software	RomCom's backdoor has a functionality to run AnyDesk application