Mar 19 2024

NETMANAGEIT

Intelligence Report
Blind Eagle's North American Journey

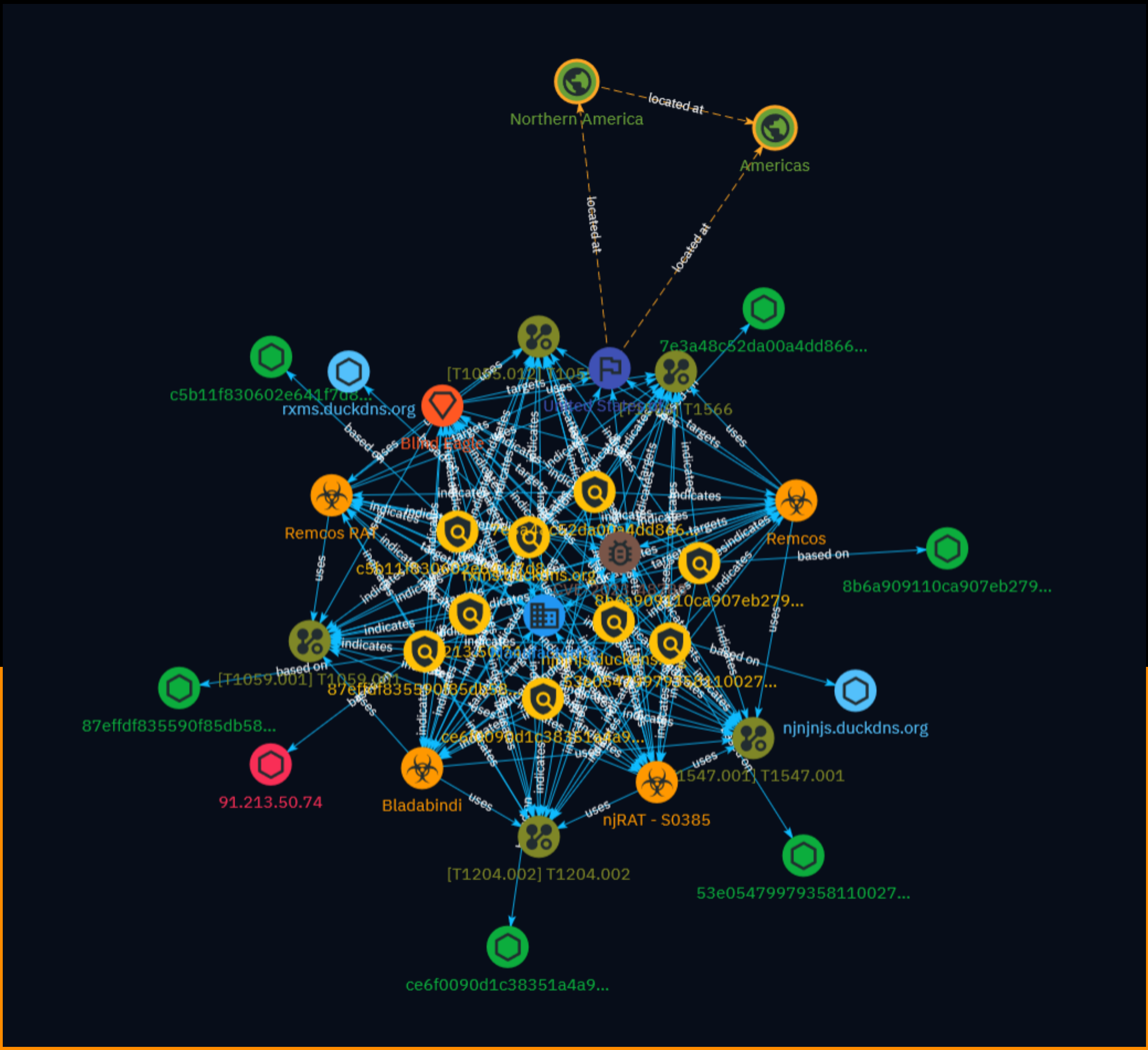

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The eSentire Threat Response Unit (TRU) recently observed the Blind Eagle threat actor targeting the manufacturing industry in North America. The actor used phishing emails containing malicious VBS files that delivered the Ande Loader, which then deployed Remcos RAT and NjRAT payloads. Technical analysis shows Blind Eagle leveraging crypters developed by threat actors known as Roda and Pjoao1578. The campaign targeted Spanish-speaking users at manufacturing companies. eSentire recommends implementing EDR solutions and security awareness training to help defend against Blind Eagle.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

rxms.duckdns.org

Pattern Type

stix

Pattern

[hostname:value = 'rxms.duckdns.org']

Name

njnjnjs.duckdns.org

Pattern Type

stix

Pattern

[hostname:value = 'njnjnjs.duckdns.org']

Name

91.213.50.74

Description
- **Zip Code:** N/A - **ISP:** IT Resheniya - **ASN:** 49943 - **Organization:** IT Resheniya - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 91.213.50.74 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RU - **Region:** Sankt-Peterburg - **City:** Saint Petersburg - **Latitude:** 59.8944397 - **Longitude:** 30.26420021
Pattern Type
stix
Pattern
[ipv4-addr:value = '91.213.50.74']
Name
ce6f0090d1c38351a4a9dab52bf4ad817c3f2ea5a6e5cef4dd139311ea1e4c54
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ce6f0090d1c38351a4a9dab52bf4ad817c3f2ea5a6e5cef4dd139311ea1e4c54']
Name
c5b11f830602e641f7d86a756da6b745d80ef6431be3f373be6912cab5f7acf5
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c5b11f830602e641f7d86a756da6b745d80ef6431be3f373be6912cab5f7acf5']

Name

8b6a909110ca907eb279cfb8f6db432af5564263e49c6982001b83fcffe04c07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b6a909110ca907eb279cfb8f6db432af5564263e49c6982001b83fcffe04c07']

Name

87effdf835590f85db589768b14adae2f76b59b2f33fae0300aef50575e6340d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87effdf835590f85db589768b14adae2f76b59b2f33fae0300aef50575e6340d']

Name

7e3a48c52da00a4dd8669103f0ba941aa824fcc097a18e7ea29f730492ba2a07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e3a48c52da00a4dd8669103f0ba941aa824fcc097a18e7ea29f730492ba2a07']

Name

53e05479979358110027cba571da6517ccb56c7ca321cf47c3ace1bbe2e1bd8d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '53e05479979358110027cba571da6517ccb56c7ca321cf47c3ace1bbe2e1bd8d']

Vulnerability

Name
CVE-2023-48788

Malware

Name
njRAT - S0385
Name
Remcos RAT
Name
Remcos
Name
Bladabindi
Description
[njRAT](https://attack.mitre.org/software/S0385) is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.(Citation: Fidelis njRAT June 2013)

Intrusion-Set

Name
Blind Eagle

Description
[APT-C-36](https://attack.mitre.org/groups/G0099) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.(Citation: QiAnXin APT-C-36 Feb2019)

Attack-Pattern

Name

T1055.012

ID

T1055.012

Description

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process. Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as `CreateProcess`, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as `ZwUnmapViewOfSection` or `NtUnmapViewOfSection` before being written to, realigned to the injected code, and resumed via `VirtualAllocEx`, `WriteProcessMemory`, `SetThreadContext`, then `ResumeThread` respectively.(Citation: Leitch Hollowing)(Citation: Elastic Process Injection July 2017) This is very similar to [Thread Local Storage](https://attack.mitre.org/techniques/T1055/005) but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

Name

T1547.001

ID

T1547.001

Description

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level. The following run keys are created by default on Windows systems: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce` Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"` (Citation: Oddvar Moe RunOnceEx Mar 2018) Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`. The following Registry keys can be used to set startup folder items for persistence: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` The following Registry keys can control automatic startup of services during boot: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` *

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices` Using policy settings to specify startup programs creates corresponding values in either of two Registry keys: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run automatically for the currently logged-on user. By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot. Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://

attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1204.002

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Country

Name
United States of America

Region

Name
Northern America

Name
Americas

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Hostname

Value
rxms.duckdns.org
njnjnjs.duckdns.org

IPv4-Addr

Value
91.213.50.74

StixFile

Value
ce6f0090d1c38351a4a9dab52bf4ad817c3f2ea5a6e5cef4dd139311ea1e4c54
c5b11f830602e641f7d86a756da6b745d80ef6431be3f373be6912cab5f7acf5
8b6a909110ca907eb279cfb8f6db432af5564263e49c6982001b83fcffe04c07
87effdf835590f85db589768b14adae2f76b59b2f33fae0300aef50575e6340d
7e3a48c52da00a4dd8669103f0ba941aa824fcc097a18e7ea29f730492ba2a07
53e05479979358110027cba571da6517ccb56c7ca321cf47c3ace1bbe2e1bd8d

External References

- https://www.esentire.com/blog/blind-eagles-north-american-journey
- https://otx.alienvault.com/pulse/65f420f93280cbf7e41d2847