Apr 04 2024

NETMANAGEIT

Intelligence Report

Bellingcat Malware Investigation

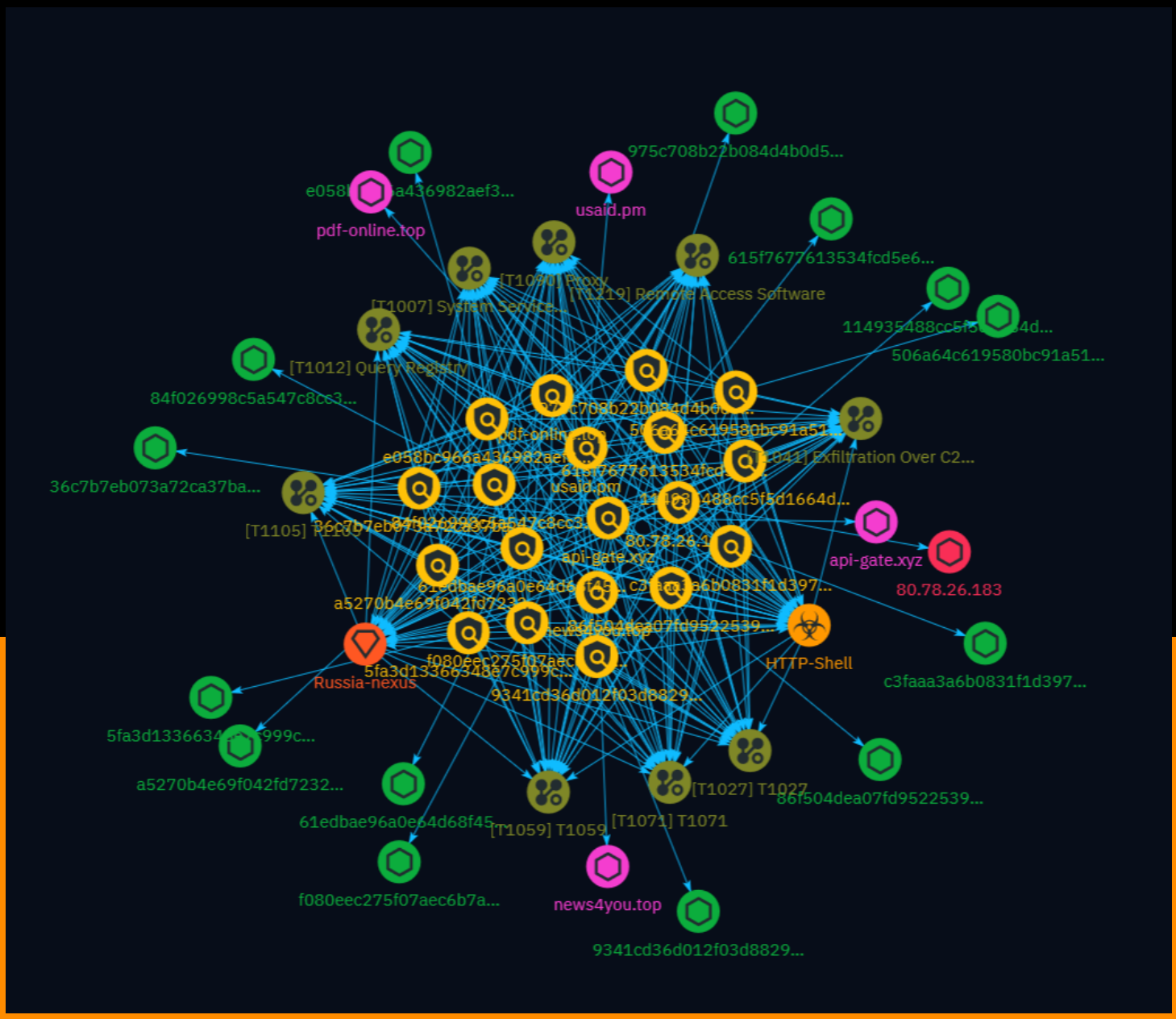

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The analysis involves an email campaign targeting the journalist group Bellingcat, delivering a malicious zip file that ultimately deploys an HTTP reverse shell. The infection chain involves a malicious zip archive, a .lnk file masquerading as a PDF, and a PowerShell script executing a reverse shell that enables data exfiltration. The campaign is attributed to a Russia-nexus threat actor based on consistent targeting of organizations critical of Russia.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

86f504dea07fd952253904c468d83d9014a290e1ff5f2d103059638e07d14b09

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86f504dea07fd952253904c468d83d9014a290e1ff5f2d103059638e07d14b09']

Name

84f026998c5a547c8cc3ba8d86d3425097c501ae85a207c121288f6c1cf72710

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '84f026998c5a547c8cc3ba8d86d3425097c501ae85a207c121288f6c1cf72710']

Name

615f7677613534fcd5e6548b4fee48fbfc85af0c5ecdad5b2046495869d1a668

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '615f7677613534fcd5e6548b4fee48fbfc85af0c5ecdad5b2046495869d1a668']

Name

usaid.pm

Pattern Type

stix

Pattern

[domain-name:value = 'usaid.pm']

Name

pdf-online.top

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1702646841, 'iso': '2023-12-15T08:27:21-05:00'} - **IPQS: Domain:** pdf-online.top - **IPQS: IP Address:** 158.160.129.176

Pattern Type

stix

Pattern

[domain-name:value = 'pdf-online.top']

Name

news4you.top

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1702646842, 'iso': '2023-12-15T08:27:22-05:00'} - **IPQS: Domain:** news4you.top - **IPQS: IP Address:** 158.160.129.176

Pattern Type

stix

Pattern

[domain-name:value = 'news4you.top']

Name

api-gate.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'api-gate.xyz']

Name

80.78.26.183

Description

- **Zip Code:** N/A - **ISP:** ab stract - **ASN:** 39287 - **Organization:** ab stract - **Is Crawler:** False - **Timezone:** Europe/Stockholm - **Mobile:** False - **Host:** 504e1ab7.host.njalla.net - **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:** SE - **Region:** Skane lan - **City:** Oxie - **Latitude:** 55.53332901 - **Longitude:** 13.10000038

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.78.26.183']

Name

f080eec275f07aec6b7a617e215d034e67e011184e1de5b2e71e441a6dd8027f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f080eec275f07aec6b7a617e215d034e67e011184e1de5b2e71e441a6dd8027f']

Name

e058bc966a436982aef3b2cbc78a380be324e80fd0789716d0c069dd441d9a48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e058bc966a436982aef3b2cbc78a380be324e80fd0789716d0c069dd441d9a48']

Name

c3faaa3a6b0831f1d3974fcee80588812ca7afeb53cc173e0b83bcb6787fa13e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c3faaa3a6b0831f1d3974fcee80588812ca7afeb53cc173e0b83bcb6787fa13e']

Name

a5270b4e69f042fd7232b2bfc529c72416a8867b282b197f4aea1045fd327921

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5270b4e69f042fd7232b2bfc529c72416a8867b282b197f4aea1045fd327921']

Name

975c708b22b084d4b0d503b4c8129d1ffee057a0636b1beed59c448dd76bbad1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '975c708b22b084d4b0d503b4c8129d1ffee057a0636b1beed59c448dd76bbad1']

Name

9341cd36d012f03d8829234a12b9ff4e0045cb233e86127ef322dc1c2bb0b585

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9341cd36d012f03d8829234a12b9ff4e0045cb233e86127ef322dc1c2bb0b585']

Name

61edbae96a0e64d68f457fdc0fc4f4a66df61436a383b8e4ea2a30d9c9c2adde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61edbae96a0e64d68f457fdc0fc4f4a66df61436a383b8e4ea2a30d9c9c2adde']

Name

506a64c619580bc91a51bde3a3c3f5aced3ed1106413ac11a721c56817b04573

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '506a64c619580bc91a51bde3a3c3f5aced3ed1106413ac11a721c56817b04573']

Name

5fa3d13366348e7c999cca9a06e4d2f5ec7f518aca3b36f0366ecedba5f2b057

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5fa3d13366348e7c999cca9a06e4d2f5ec7f518aca3b36f0366ecedba5f2b057']

Name

36c7b7eb073a72ca37bab88b242cdadfc3cd5da7b4f714004bc63cdcee331970

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36c7b7eb073a72ca37bab88b242cdadfc3cd5da7b4f714004bc63cdcee331970']

Name

114935488cc5f5d1664dbc4c305d97a7d356b0f6d823e282978792045f1c7ddb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '114935488cc5f5d1664dbc4c305d97a7d356b0f6d823e282978792045f1c7ddb']

Malware

Name
HTTP-Shell

Intrusion-Set

Name
Russia-nexus

Attack-Pattern

Name
Query Registry
ID
T1012
Description
Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Name
Exfiltration Over C2 Channel
ID
T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to

open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems.

For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Remote Access Software

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)).

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

StixFile

Value
86f504dea07fd952253904c468d83d9014a290e1ff5f2d103059638e07d14b09
84f026998c5a547c8cc3ba8d86d3425097c501ae85a207c121288f6c1cf72710
615f7677613534fcd5e6548b4fee48fbfc85af0c5ecdad5b2046495869d1a668
f080eec275f07aec6b7a617e215d034e67e011184e1de5b2e71e441a6dd8027f
e058bc966a436982aef3b2cbc78a380be324e80fd0789716d0c069dd441d9a48
c3faaa3a6b0831f1d3974fcee80588812ca7afeb53cc173e0b83bcb6787fa13e
a5270b4e69f042fd7232b2bfc529c72416a8867b282b197f4aea1045fd327921
975c708b22b084d4b0d503b4c8129d1ffee057a0636b1beed59c448dd76bbad1
9341cd36d012f03d8829234a12b9ff4e0045cb233e86127ef322dc1c2bb0b585
5fa3d13366348e7c999cca9a06e4d2f5ec7f518aca3b36f0366ecedba5f2b057
61edbae96a0e64d68f457fdc0fc4f4a66df61436a383b8e4ea2a30d9c9c2adde
36c7b7eb073a72ca37bab88b242cdadfc3cd5da7b4f714004bc63cdcee331970
114935488cc5f5d1664dbc4c305d97a7d356b0f6d823e282978792045f1c7ddb

506a64c619580bc91a51bde3a3c3f5aced3ed1106413ac11a721c56817b04573

Domain-Name

Value
usaid.pm
pdf-online.top
api-gate.xyz
news4you.top

IPv4-Addr

Value
80.78.26.183

External References

- https://intelcorgi.com/2024/03/24/bellingcat-malware-investigation
- https://otx.alienvault.com/pulse/660b12585f85ac62a6acde45