Apr 19 2024

NETMANAGEIT

Intelligence Report

Kapeka: A novel backdoor spotted in Eastern Europe

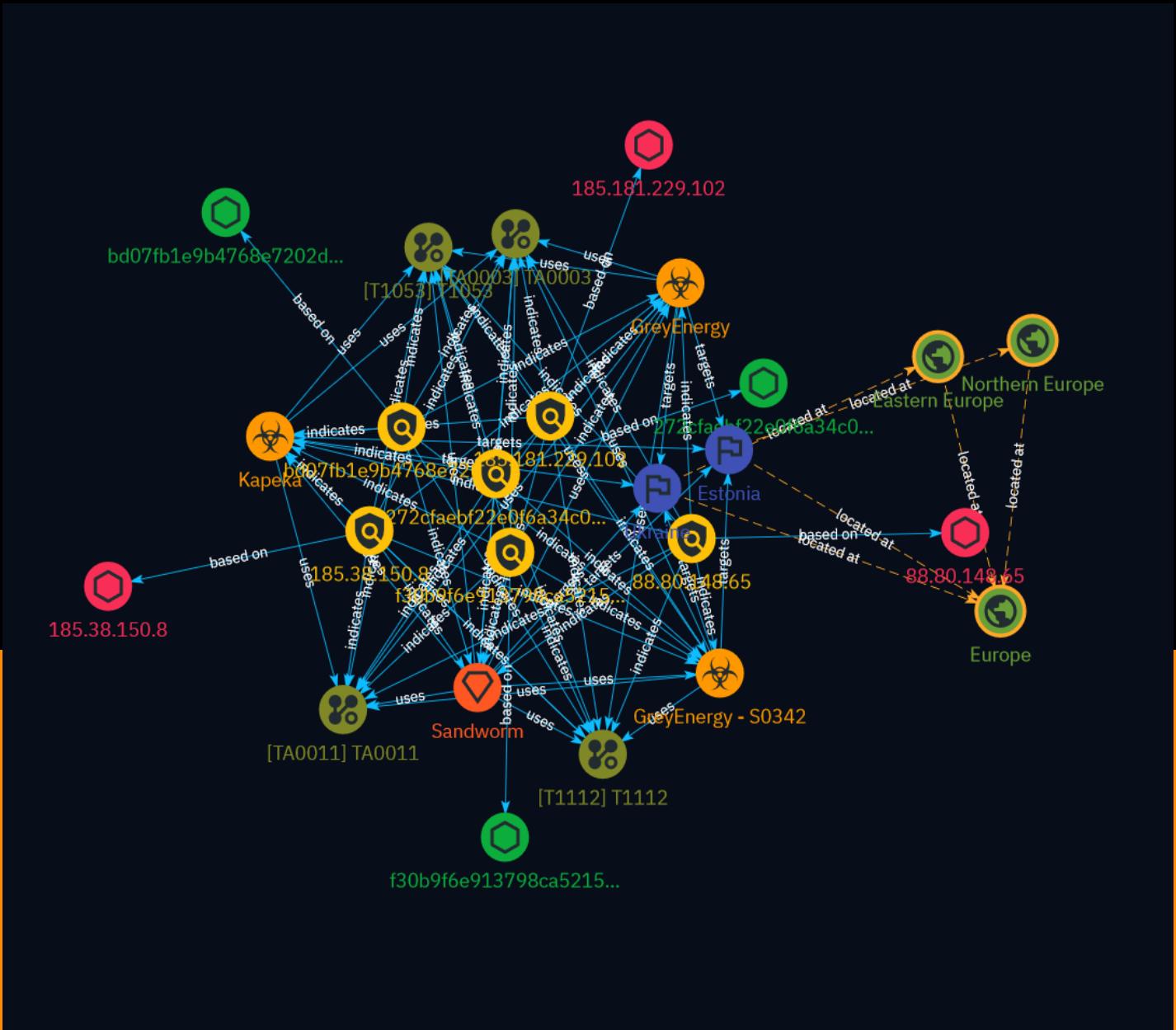

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In mid-2023 WithSecure found several artifacts observed in an intrusion set likely linked to Russian APT activity. One of these artifacts was an unknown backdoor/dropper detected in an Estonian logistics company in late 2022. Upon analysis, WithSecure found two additional versions of the dropped backdoor submitted to VirusTotal from Ukraine in mid-2022 and mid-2023, one of which was packaged with a scheduled task file from an infected machine that launched the backdoor.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

f30b9f6e913798ca52154c88725ee262a7bf92fe7caac1ae2e5147e457b9b08a

Description

stack_string SHA256 of 9bbde40cab30916b42e59208fbcc09affef525c1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f30b9f6e913798ca52154c88725ee262a7bf92fe7caac1ae2e5147e457b9b08a']

Name

bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db1386c3f

Description

stack_string SHA256 of 80fb042b4a563efe058a71a647ea949148a56c7c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db1386c3f']

Name

272cfaebf22e0f6a34c0a93b7c9c5b67c725947ba0f17e60ed67dbf6e1602043

Description

stack_string SHA256 of 97e0e161d673925e42cdf04763e7eaa53035338b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '272cfaebf22e0f6a34c0a93b7c9c5b67c725947ba0f17e60ed67dbf6e1602043']

Name

88.80.148.65

Description

- **Zip Code:** N/A - **ISP:** Belcloud - **ASN:** 44901 - **Organization:** Belcloud - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 88.80.148.65 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Sofia-Capital - **City:** Sofia - **Latitude:** 42.68000031 - **Longitude:** 23.31999969

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.80.148.65']

Name

185.38.150.8

Description

- **Zip Code:** N/A - **ISP:** Hydra Communications - **ASN:** 25369 - **Organization:** Hydra Communications - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** 8.150.38.185.baremetal.zare.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** London - **Latitude:** 51.50999832 - **Longitude:** -0.09

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.38.150.8']

Name

185.181.229.102

Description

- **Zip Code:** N/A - **ISP:** IP HOST Data Center - **ASN:** 60602 - **Organization:** Surfshark VPN - **Is Crawler:** False - **Timezone:** Europe/Chisinau - **Mobile:** False - **Host:** no-rdns.innovahosting.net - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MD - **Region:** Chiinu Municipality - **City:** Chisinau - **Latitude:** 47.00999832 - **Longitude:** 28.86000061

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.181.229.102']

Malware

Name
GreyEnergy - S0342
Name
Kapeka
Name
GreyEnergy
Description
[GreyEnergy](https://attack.mitre.org/software/S0342) is a backdoor written in C and compiled in Visual Studio. [GreyEnergy](https://attack.mitre.org/software/S0342) shares similarities with the [BlackEnergy](https://attack.mitre.org/software/S0089) malware and is thought to be the successor of it.(Citation: ESET GreyEnergy Oct 2018)

Attack-Pattern

Name
TA0011
ID
TA0011
Name
TA0003
ID
TA0003
Name
T1112
ID
T1112
Description
Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other

techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Intrusion-Set

Name
Sandworm

Country

Name
Estonia

Name
Ukraine

Region

Name
Northern Europe
Name
Eastern Europe
Name
Europe

StixFile

Value
f30b9f6e913798ca52154c88725ee262a7bf92fe7caac1ae2e5147e457b9b08a
bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db1386c3f
272cfaebf22e0f6a34c0a93b7c9c5b67c725947ba0f17e60ed67dbf6e1602043

IPv4-Addr

Value
88.80.148.65
185.38.150.8
185.181.229.102

External References

- https://labs.withsecure.com/publications/kapeka
- https://otx.alienvault.com/pulse/662121029d1dc4deba414fae