Aug 10 2023

NETMANAGEIT

Intelligence Report

Focus on DroxiDat/ SystemBC

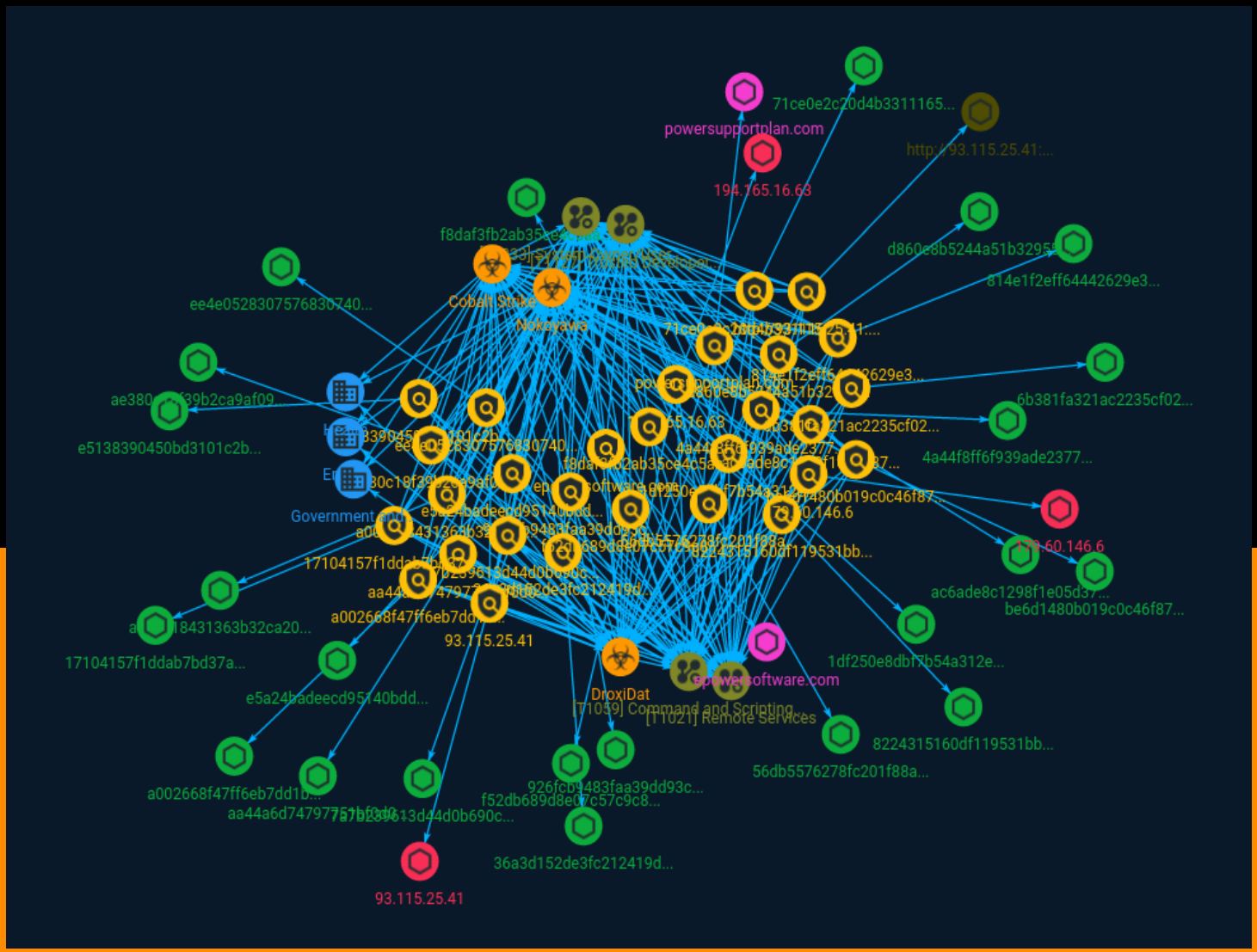

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Kaspersky's research into industrial ransomware shows that the threat posed by cybercrime groups is increasing, particularly in the area of electric utility networks, especially in south-east South Africa.

Confidence

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

15 / 100

Indicator

Name
8224315160df119531bb2255b8850150b3a2f0dfee168a9b290fe5c46b6d7ccc
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8224315160df119531bb2255b8850150b3a2f0dfee168a9b290fe5c46b6d7ccc']
Name
36a3d152de3fc212419d2733c000b17d143dfb1cf351c416b1713ef661f898b5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '36a3d152de3fc212419d2733c000b17d143dfb1cf351c416b1713ef661f898b5']
Name

71ce0e2c20d4b33111651477862cd86ab54c1a772c4b6c7125b3a35cab8dea70

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71ce0e2c20d4b33111651477862cd86ab54c1a772c4b6c7125b3a35cab8dea70']

Name

f52db689d8e07c57c9c884175fc6687237bf05adcba75727bc6f47c9c6870482

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f52db689d8e07c57c9c884175fc6687237bf05adcba75727bc6f47c9c6870482']

Name

a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e']

Name

1df250e8dbf7b54a312eb55a55551537567c793933b25ad8f3f801c1dd3e8b95

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1df250e8dbf7b54a312eb55a55551537567c793933b25ad8f3f801c1dd3e8b95']

Name

56db5576278fc201f88ae69389fb59df55881de2e090f76f36bfb8bb34cd17af

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '56db5576278fc201f88ae69389fb59df55881de2e090f76f36bfb8bb34cd17af']

Name

epowersoftware.com

Pattern Type

stix

Pattern

[domain-name:value = 'epowersoftware.com']

Name

d860e8b5244a51b329556faafe93096d41d40d119751f088af67225383ef4980

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd860e8b5244a51b329556faafe93096d41d40d119751f088af67225383ef4980']

Name

aa44a6d74797751bf0d021ea8e746d7bf92ed5bfd1dbab687a82bad85cfb0813

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa44a6d74797751bf0d021ea8e746d7bf92ed5bfd1dbab687a82bad85cfb0813']

Name

ac6ade8c1298f1e05d37f904ee65615c0367ebd764b2d23be2acf4a8d367547d

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ac6ade8c1298f1e05d37f904ee65615c0367ebd764b2d23be2acf4a8d367547d']
Name
4a44f8ff6f939ade23774689745f141ed5a77f5804067358a6d4f7876ce393eb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4a44f8ff6f939ade23774689745f141ed5a77f5804067358a6d4f7876ce393eb']
Name
926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732']

Name
814e1f2eff64442629e318e5e398d17a59dc067b1d7006bf85d7f74309635f5b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '814e1f2eff64442629e318e5e398d17a59dc067b1d7006bf85d7f74309635f5b']
Name
7a7b239613d44d0b690cee93022de0a4171fc2040e6eafd6002fbd4a77f1685b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7a7b239613d44d0b690cee93022de0a4171fc2040e6eafd6002fbd4a77f1685b']
Name
194.165.16.63
Description
CC=MC ASN=AS48721 Flyservers S.A.
Pattern Type

stix

Pattern

[ipv4-addr:value = '194.165.16.63']

Name

179.60.146.6

Description

CC=RU ASN=AS42237 w1n ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.60.146.6']

Name

a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4']

Name

powersupportplan.com

Pattern Type

stix

Pattern

[domain-name:value = 'powersupportplan.com']

Name

93.115.25.41

Description

ISP: UAB Cherry Servers **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Tue, 01 Aug 2023 01:56:34 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Thu, 23 Feb 2023 02:53:29 GMT ETag: "2aa6-5f5551e1ac897" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -23 rootdelay: 0.00715637207031 rootdisp: 0.0221710205078 refid: 85196821 reftime: 3899794238.76 poll: 3 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.115.25.41']

Name

e5138390450bd3101c2b39c99eadf424eee6c0566fedb8815a86c4f46e39366e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e5138390450bd3101c2b39c99eadf424eee6c0566fedb8815a86c4f46e39366e']

Name

be6d1480b019c0c46f87eb3b54eb2857d10aa11f8cf438af5c99fa2c164b52fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'be6d1480b019c0c46f87eb3b54eb2857d10aa11f8cf438af5c99fa2c164b52fc']

Name

17104157f1ddab7bd37a1cf56c9c324935c615f0206ce8f38a1f93e4abe9bd90

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17104157f1ddab7bd37a1cf56c9c324935c615f0206ce8f38a1f93e4abe9bd90']

Name

http://93.115.25.41:443

Pattern Type

stix

Pattern

[url:value = 'http://93.115.25.41:443']

Name

f8daf3fb2ab35ce4c5aa5f04f34283d737c0cc30a29ab8ee1ec1aca487e8f9c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8daf3fb2ab35ce4c5aa5f04f34283d737c0cc30a29ab8ee1ec1aca487e8f9c3']

Name

ae380c18f39b2ca9af09e83c7aeaa59a2f74692c62eb6d0d907fd650eb8682e6

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = 'ae380c18f39b2ca9af09e83c7aeaa59a2f74692c62eb6d0d907fd650eb8682e6']
Name
6b381fa321ac2235cf023201dccce72253376d53d48d685d27404b60c8890fff
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6b381fa321ac2235cf023201dccce72253376d53d48d685d27404b60c8890fff']
Name
ee4e05283075768307400 57e6f9656c293d71ba8856ab4e5fadbca87eb2b94e1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ee4e05283075768307400 57e6f9656c293d71ba8856ab4e5fadbca87eb2b94e1']
Name
e5a24badeecd95140bddff4bb668aca96f33c9b5fc870cdbbd3a9092e809a4ea

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'e5a24badeecd95140bddff4bb668aca96f33c9b5fc870cdbbd3a9092e809a4ea']

Malware

Name
DroxiDat
Name
Nokoyawa
Name
Cobalt Strike
Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Attack-Pattern

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Name

Command and Scripting Interpreter

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

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands

may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple

Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Sector

Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Domain-Name

Value
epowersoftware.com
powersupportplan.com

StixFile

Value
7a7b239613d44d0b690cee93022de0a4171fc2040e6eafd6002fbd4a77f1685b
f52db689d8e07c57c9c884175fc6687237bf05adcba75727bc6f47c9c6870482
814e1f2eff64442629e318e5e398d17a59dc067b1d7006bf85d7f74309635f5b
ac6ade8c1298f1e05d37f904ee65615c0367ebd764b2d23be2acf4a8d367547d
f8daf3fb2ab35ce4c5aa5f04f34283d737c0cc30a29ab8ee1ec1aca487e8f9c3
8224315160df119531bb2255b8850150b3a2f0dfee168a9b290fe5c46b6d7ccc
a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4
4a44f8ff6f939ade23774689745f141ed5a77f5804067358a6d4f7876ce393eb
36a3d152de3fc212419d2733c000b17d143dfb1cf351c416b1713ef661f898b5
e5138390450bd3101c2b39c99eadf424eee6c0566fedb8815a86c4f46e39366e
56db5576278fc201f88ae69389fb59df55881de2e090f76f36bfb8bb34cd17af
e5a24badeecd95140bddff4bb668aca96f33c9b5fc870cdbbd3a9092e809a4ea
ae380c18f39b2ca9af09e83c7aeaa59a2f74692c62eb6d0d907fd650eb8682e6

6b381fa321ac2235cf023201dccce72253376d53d48d685d27404b60c8890fff

a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e

71ce0e2c20d4b33111651477862cd86ab54c1a772c4b6c7125b3a35cab8dea70

aa44a6d74797751bf0d021ea8e746d7bf92ed5bfd1dbab687a82bad85cfb0813

d860e8b5244a51b329556faafe93096d41d40d119751f088af67225383ef4980

be6d1480b019c0c46f87eb3b54eb2857d10aa11f8cf438af5c99fa2c164b52fc

1df250e8dbf7b54a312eb55a55551537567c793933b25ad8f3f801c1dd3e8b95

ee4e0528307576830740057e6f9656c293d71ba8856ab4e5fadbca87eb2b94e1

926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732

17104157f1ddab7bd37a1cf56c9c324935c615f0206ce8f38a1f93e4abe9bd90

IPv4-Addr

Value
194.165.16.63
93.115.25.41
179.60.146.6

Url

Value
http://93.115.25.41:443

External References

- https://otx.alienvault.com/pulse/64d5587d8a1c7dae958a6a3f
- https://securelist.com/focus-on-droxidat-systembc/110302/