Oct 29 2023

NETMANAGEIT

Intelligence Report

Crambus: New Campaign Targets Middle Eastern Government

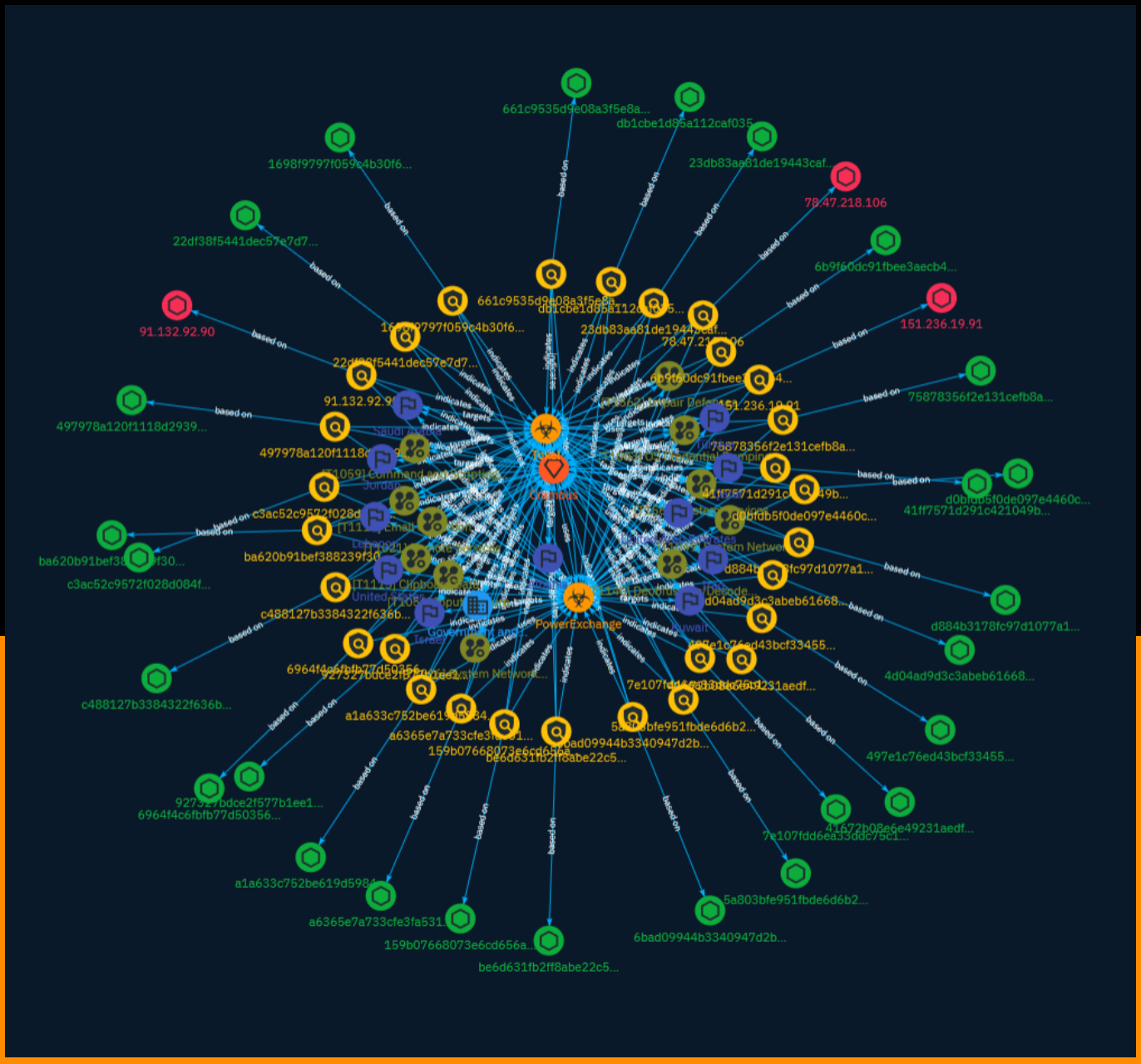

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A long-running Iranian espionage group staged an eight-month cyber attack against a government in the Middle East, according to a report from security firm Symantec, which assessed the extent of the attack.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various

different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Impair Defenses

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Name

System Network Configuration Discovery

ID

T1016

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

Email Collection

ID

T1114

Description

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

Name

System Services

ID

T1569

Description

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or Modify System Process](https://attack.mitre.org/techniques/T1543)), but adversaries can also abuse services for one-time or temporary execution.

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

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)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name
6bad09944b3340947d2b39640b0e04c7b697a9ce70c7e47bc2276ed825e74a2a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6bad09944b3340947d2b39640b0e04c7b697a9ce70c7e47bc2276ed825e74a2a']
Name
22df38f5441dec57e7d7c2e1a38901514d3f55203b2890dc38d2942f1e4bc100
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '22df38f5441dec57e7d7c2e1a38901514d3f55203b2890dc38d2942f1e4bc100']
Name

23db83aa81de19443cafe14c9c0982c511a635a731d6df56a290701c83dae9c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23db83aa81de19443cafe14c9c0982c511a635a731d6df56a290701c83dae9c7']

Name

927327bdce2f577b1ee19aa3ef72c06f7d6c2ecd5f08acc986052452a807caf2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '927327bdce2f577b1ee19aa3ef72c06f7d6c2ecd5f08acc986052452a807caf2']

Name

6964f4c6fbfb77d50356c2ee944f7ec6848d93f05a35da6c1acb714468a30147

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6964f4c6fbfb77d50356c2ee944f7ec6848d93f05a35da6c1acb714468a30147']

Name

7e107fdd6ea33ddc75c1b75fdf7a99d66e4739b4be232ff5574bf0e116bc6c05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e107fdd6ea33ddc75c1b75fdf7a99d66e4739b4be232ff5574bf0e116bc6c05']

Name

ba620b91bef388239f3078ecdcc9398318fd8465288f74b4110b2a463499ba08

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba620b91bef388239f3078ecdcc9398318fd8465288f74b4110b2a463499ba08']

Name

78.47.218.106

Description

CC=DE ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '78.47.218.106']

Name

41672b08e6e49231aedf58123a46ed7334cafaad054f2fd5b1e0c1d5519fd532

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41672b08e6e49231aedf58123a46ed7334cafaad054f2fd5b1e0c1d5519fd532']

Name

c488127b3384322f636b2a213f6f7b5fdaa6545a27d550995dbf3f32e22424bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c488127b3384322f636b2a213f6f7b5fdaa6545a27d550995dbf3f32e22424bf']

Name

6b9f60dc91fbee3aecb4a875e24af38c97d3011fb23ace6f34283a73349c4681

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6b9f60dc91fbee3aecb4a875e24af38c97d3011fb23ace6f34283a73349c4681']

Name

a6365e7a733cfe3fa5315d5f9624f56707525bbf559d97c66dbe821fae83c9e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6365e7a733cfe3fa5315d5f9624f56707525bbf559d97c66dbe821fae83c9e9']

Name

75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372']

Name

d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae']

Name

a1a633c752be619d5984d02d4724d9984463aa1de0ea1375efda29cadb73355a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a1a633c752be619d5984d02d4724d9984463aa1de0ea1375efda29cadb73355a']

Name

151.236.19.91

Description

CC=GB ASN=AS39326 HighSpeed Office Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '151.236.19.91']

Name

5a803bfe951fbde6d6b23401c4fd1267b03f09d3907ef83df6cc25373c11a11a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a803bfe951fbde6d6b23401c4fd1267b03f09d3907ef83df6cc25373c11a11a']

Name

91.132.92.90

Description

ISP: M247 Europe SRL **OS:** None ---------- Hostnames: - 90.92.132.91.in-addr.arpa ---------- Domains: - 91.in-addr.arpa ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC6cenxKHN+hFkKZdrcR03SrKdkAaJmkO96OF5Cy17sel//X8xGUrJbcC1jwkoC9r+DsLf62t8lrQSbuSkYFkG4ECawgP21b5zX0aNubU2MAek4hfn9n/2wZk4NmHdubdLj3ngqoqchj00kdZm8HSWmrv5P5GxhF3ak8O84+CXk9u50RHAF0/DpFJUHvOwVnZq3fwTv tDVYNasZHMnG+Gjbo5A7Vl90RkIx/

LEhd3AWvNGXoVx2nBej80IYS147sDDWrcdA7vkib/8CkyR4
CZr6jNbaWeQIXdkuN8Ei7elqDhIWG3P6noGku1kC39REoFnKcCytTBC2t267m34A26EYwWjMw+jU
26G8rGMJeM+E6GA1uQWDZp2t52Q+z2vLteJpuXUaUqNFZq7kaydpuUsVfupZu3DHBWsgmG6DW
nRT 5sKsKi5F9bqotLev7gSbci2UTwWgYuOF+SC7QXiRb+biIZs7mKFuEcGLFIQR+5qTK6HvodqNV/
Lc uopkTEpkacM= Fingerprint: 96:12:a0:23:2f:e8:85:a0:e0:20:8c:d1:46:4c:9c:78 Kex Algorithms:
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384
ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512
diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms:
rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms:
chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-
gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression
Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` SSH-2.0-OpenSSH_8.2p1
Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAABgQC6cenxKHN+hFkKZdrcR03SrKdkAaJmkO96OF5Cy17sel//
X8xGUrJbcC1jwkoC9r+DsLf62t8lrQSbuSkYFkG4ECawgP21b5zX0aNubU2MAek4hfn9n/2wZk4N
mHdubdLj3ngqoqchj00kdZm8HSWmrv5P5GxhF3ak8O84+CXk9u50RHAF0/
DpFJUHvOwVnZq3fwTv tDVYNasZHMnG+Gjbo5A7Vl90RkIx/
LEhd3AWvNGXoVx2nBej80IYS147sDDWrcdA7vkib/8CkyR4
CZr6jNbaWeQIXdkuN8Ei7elqDhIWG3P6noGku1kC39REoFnKcCytTBC2t267m34A26EYwWjMw+jU
26G8rGMJeM+E6GA1uQWDZp2t52Q+z2vLteJpuXUaUqNFZq7kaydpuUsVfupZu3DHBWsgmG6DW
nRT 5sKsKi5F9bqotLev7gSbci2UTwWgYuOF+SC7QXiRb+biIZs7mKFuEcGLFIQR+5qTK6HvodqNV/
Lc uopkTEpkacM= Fingerprint: 96:12:a0:23:2f:e8:85:a0:e0:20:8c:d1:46:4c:9c:78 Kex Algorithms:
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384
ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512
diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms:
rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms:
chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-
gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression
Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.132.92.90']

Name

4d04ad9d3c3abeb61668e52a52a37a46c1a60bc8f29f12b76ff9f580caeefba8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d04ad9d3c3abeb61668e52a52a37a46c1a60bc8f29f12b76ff9f580caeefba8']

Name

159b07668073e6cd656ad7e3822db997d5a8389a28c439757eb60ba68eaff70f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '159b07668073e6cd656ad7e3822db997d5a8389a28c439757eb60ba68eaff70f']

Name

661c9535d9e08a3f5e8ade7c31d5017519af2101786de046a4686bf8a5a911ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '661c9535d9e08a3f5e8ade7c31d5017519af2101786de046a4686bf8a5a911ff']

Name

497e1c76ed43bcf334557c64e1a9213976cd7df159d695dcc19c1ca3d421b9bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '497e1c76ed43bcf334557c64e1a9213976cd7df159d695dcc19c1ca3d421b9bc']

Name

1698f9797f059c4b30f636d16528ed3dd2b4f8290e67eb03e26181e91a3d7c3b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1698f9797f059c4b30f636d16528ed3dd2b4f8290e67eb03e26181e91a3d7c3b']

Name

41ff7571d291c421049bfbd8d6d3c51b0a380db3b604cef294c1edfd465978d9

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '41ff7571d291c421049bfbd8d6d3c51b0a380db3b604cef294c1edfd465978d9']
Name
be6d631fb2ff8abe22c5d48035534d0dede4abfd8c37b1d6cbf61b005d1959c1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'be6d631fb2ff8abe22c5d48035534d0dede4abfd8c37b1d6cbf61b005d1959c1']
Name
c3ac52c9572f028d084f68f6877bf789204a6a0495962a12ee2402f66394a918
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c3ac52c9572f028d084f68f6877bf789204a6a0495962a12ee2402f66394a918']

Name

d0bfdb5f0de097e4460c13bc333755958fb30d4cb22e5f4475731ad1bdd579ec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0bfdb5f0de097e4460c13bc333755958fb30d4cb22e5f4475731ad1bdd579ec']

Name

497978a120f1118d293906524262da64b15545ee38dc0f6c10dbff3bd9c0bac2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '497978a120f1118d293906524262da64b15545ee38dc0f6c10dbff3bd9c0bac2']

Name

db1cbe1d85a112caf035fd5d4babfb59b2ca93411e864066e60a61ec8fe27368

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'db1cbe1d85a112caf035fd5d4babfb59b2ca93411e864066e60a61ec8fe27368']
```

Intrusion-Set

Name
Crambus

Country

Name
United Arab Emirates
Name
Lebanon
Name
Qatar
Name
Israel
Name
Saudi Arabia
Name
Kuwait
Name
United States

Name
Türkiye
Name
Albania
Name
Jordan
Name
Iraq

Malware

Name
PowerExchange

Name
Tokel

StixFile

Value
a1a633c752be619d5984d02d4724d9984463aa1de0ea1375efda29cadb73355a
6b9f60dc91fbee3aecb4a875e24af38c97d3011fb23ace6f34283a73349c4681
d0bfdb5f0de097e4460c13bc333755958fb30d4cb22e5f4475731ad1bdd579ec
41ff7571d291c421049bfbd8d6d3c51b0a380db3b604cef294c1edfd465978d9
23db83aa81de19443cafe14c9c0982c511a635a731d6df56a290701c83dae9c7
497e1c76ed43bcf334557c64e1a9213976cd7df159d695dcc19c1ca3d421b9bc
927327bdce2f577b1ee19aa3ef72c06f7d6c2ecd5f08acc986052452a807caf2
22df38f5441dec57e7d7c2e1a38901514d3f55203b2890dc38d2942f1e4bc100
6bad09944b3340947d2b39640b0e04c7b697a9ce70c7e47bc2276ed825e74a2a
d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae
5a803bfe951fbde6d6b23401c4fd1267b03f09d3907ef83df6cc25373c11a11a
c488127b3384322f636b2a213f6f7b5fdaa6545a27d550995dbf3f32e22424bf
be6d631fb2ff8abe22c5d48035534d0dede4abfd8c37b1d6cbf61b005d1959c1

a6365e7a733cfe3fa5315d5f9624f56707525bbf559d97c66dbe821fae83c9e9

497978a120f1118d293906524262da64b15545ee38dc0f6c10dbff3bd9c0bac2

159b07668073e6cd656ad7e3822db997d5a8389a28c439757eb60ba68eaff70f

6964f4c6fbfb77d50356c2ee944f7ec6848d93f05a35da6c1acb714468a30147

661c9535d9e08a3f5e8ade7c31d5017519af2101786de046a4686bf8a5a911ff

41672b08e6e49231aedf58123a46ed7334cafaad054f2fd5b1e0c1d5519fd532

7e107fdd6ea33ddc75c1b75fdf7a99d66e4739b4be232ff5574bf0e116bc6c05

1698f9797f059c4b30f636d16528ed3dd2b4f8290e67eb03e26181e91a3d7c3b

4d04ad9d3c3abeb61668e52a52a37a46c1a60bc8f29f12b76ff9f580caeefba8

ba620b91bef388239f3078ecdcc9398318fd8465288f74b4110b2a463499ba08

75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372

c3ac52c9572f028d084f68f6877bf789204a6a0495962a12ee2402f66394a918

db1cbe1d85a112caf035fd5d4babfb59b2ca93411e864066e60a61ec8fe27368

IPv4-Addr

Value
151.236.19.91
91.132.92.90
78.47.218.106

External References

- https://otx.alienvault.com/pulse/6532fc649fb565be22515704
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government