THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Pay2Key.I2P

Ransomware-as-a-Service (RaaS) Campaign

CATEGORY

Malware Campaign

SEVERITY

High

Platforms

Windows

IMPACT

- Operational Disruption
- Financial Losses
- Data Exposure
- Security Control Evasion
- Cross-Platform Threats

Description

Pay2Key.I2P Ransomware-as-a-Service (RaaS) Campaign

In the wake of heightened geopolitical tensions involving Israel, Iran, and the United States, a sophisticated ransomware campaign has resurfaced, affecting organizations across Western regions. Identified as Pay2Key.I2P, this Ransomware-as-a-Service (RaaS) operation exhibits ties to the Iranian-linked Fox Kitten APT group and integrates characteristics of the previously reported Mimic ransomware (ELENOR-Corp variant).

Pay2Key.I2P affiliates are incentivized with an 80% profit share up from a prior 70% for executing attacks aligned with Iranian interests. The operation has reportedly amassed over $4 million in ransom payments in just four months, highlighting the growing threat posed by ideologically and financially motivated threat actors.

Technical Summary:

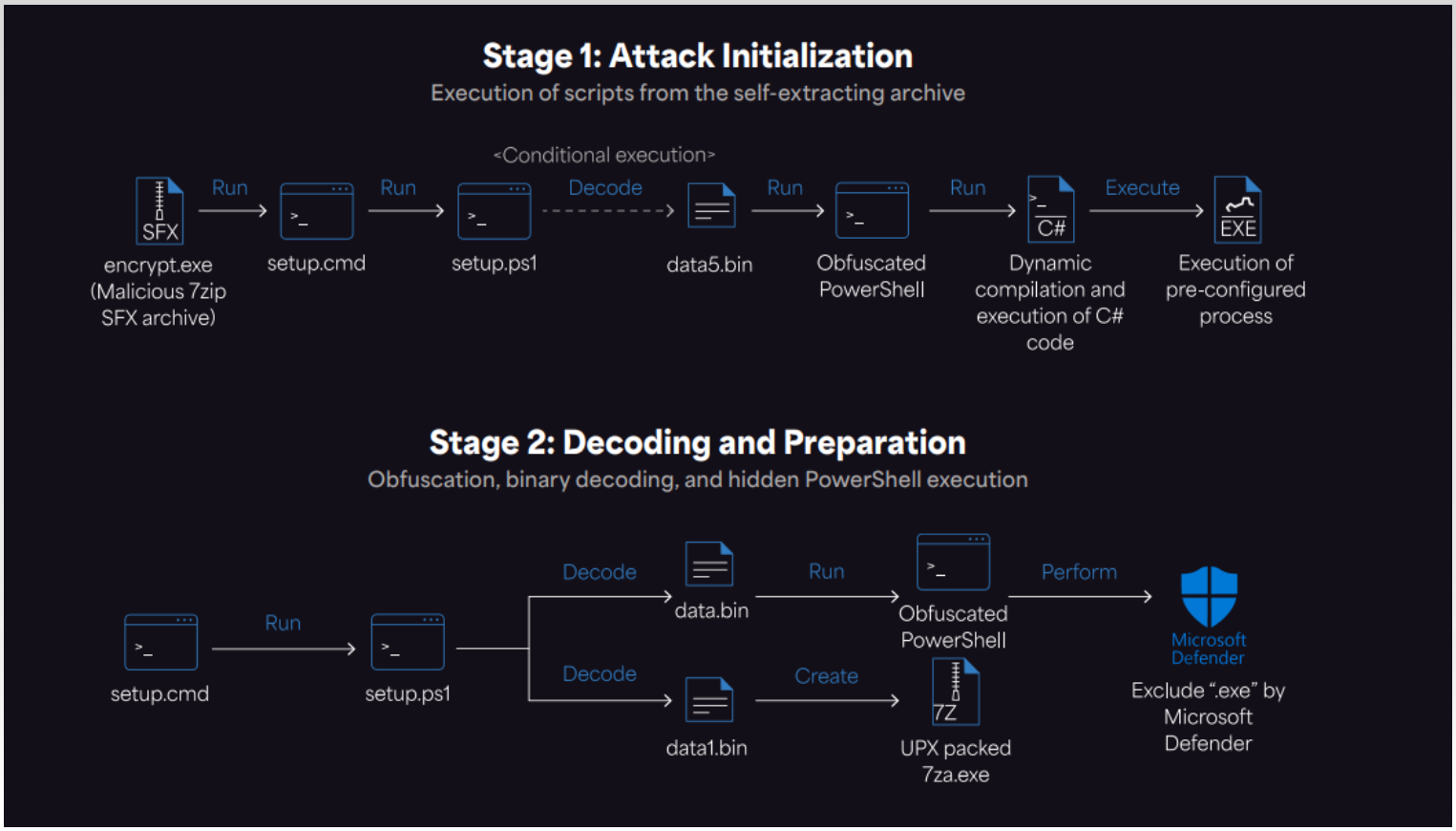
Delivery Method:

- Distributed as a 7-Zip Self-Extracting (SFX) archive
- Executes a batch file (setup.cmd) upon extraction
- Utilizes obfuscated PowerShell scripts to disable Microsoft Defender and drop payloads

Payload Components:

- powrprof.exe: Disguised NoDefender utility
- enc-build.exe: Protected ransomware binary (linked to Mimic)
- Everything.exe suite: File indexer and associated configuration files
- wsc_proxy.exe, wsc.dll: Avast-signed binaries exploited for AV evasion

Infection chain and technical analysis



Indicator of Compromise

SHA-256

2fefb69e4b2310be5e09d329e8cf1bebd1f9e18884c8c2a38af8d7ea46bd5e01
89ad2164717bd5f5f93fbb4cebf0efeb473097408fddfc7fc7b924d790514dc5
3ba64d08edbfadec8e301673df8b36f9f7475c83587930fc9577ea366ec06839
39d3ba87a27eae69a01666b0ecbb8c60259be4b3decf4cdd1d950c98c6c0b08c
60ec008c8515934c3c8d89f84bbcc8fac9144e642c0143d8230f465f4e66f62c
a05c18e81911608cf2edb19907092d542548abb695e48e3217dfbec2f3dfcd04
d8e423c8644b686ad3376f38f3e4df55a152ee4cac2af3079651263f002d8c26
9c06ea83553c6dab3d831e1046cee237a9c1b1ed79b3b2e37ed9f3c8a38643eb
242fa471582c2f37c17717dc260cb108584c44e86b8831382f7b2f5fc63aeb6b
7336b865f232f7fccb9b85524d5ebdc444344de363f77e1b1c3eaeeb3428e1a5
1d0ec8e34703a7589533462be62c020004cfe0f7b20204f9e6c79b84cbfafc9b
d61a55d368a1dcf570f633c7a23ae12361749c2d7000178dd9e353528c325907
17fc4df8ef9a92c972684cba707c3976b91bcd7f0251f42f1b63e4de0e688d6c
b64305852ddb317b7839b39db602fcdda60e7658f391ff4ba52fce4dbca89089
1c70d4280835f18654422cec1b209eec856f90344b8f02afca82716555346a55
a8bfa1389c49836264cfa31fc4410b88897a78d9c2152729d28eca8c12171b9e
1c3f2530b2764754045039066d2c277dff4efabd4f15f2944e30b10e82f443c0
bd4635d582413f84ac83adbb4b449b18bac4fc87ca000d0c7be84ad0f9caf68e
fb653fd840b0399cea31986b49b5ceadd28fb739dd2403a8bb05051eea5e5bbc

SHA-1

c452d8d4c3a82af4bc57ca8a76e4407aaf90deca
204e6a57c44242fad874377851b13099dfe60176
7abce96681b4a74a67be918ab655e8a52040c128
a4a278510494b19d552f4c3e76e5d05e148a3d5f
aed74c166d431452388bf0eb64aef6484608bac3
dec61ce5d513e93aaa5610986bb1214a89e21ae2
ac8165b04b7a06da9a025fee2db3ee67343667f1
f9e31e0b9443dba41c26fce80fd6b509426ee39b
fcddc56a81048f991dd692814d41d32a3b53a16c
505aa739c467e6bcc41220baf9c6f16ea8c8bea8
8e4d426e76afe5ef7a051a9b2a8f00bb671687de
9b391b848823513870f8f95fc6a6ae4456b306fb
2e27f78c4e48f39a207701a63f6aff12f864d920
b60dbc07b2adca040060d1c21e840861739477c5
ccea8b21373642983ca4e26c9099c45d2f03c258
e31d3daf4eb105079390b16d096f783ed7457435
fbfdc8bbff6225cebcc4f005c985159096b0d709
ff2d55a844c1fd37b3841cefa7e2d21de5fa8bac
c79bddbea392247a4e88221f53c0e2e30368b614

Indicator of Compromise

MD5

742c2400f2de964d0cce4a8dabadd708
51014c0c06acdd80f9ae4469e7d30a9e
45ddf68aa972951e22fad44817ee4e17
9b1e88aa2f45c2f6d4b43f2208bf816b
f738883b4c7ccaeb1008d013402b5021
2193c638919b394837332257a1219199
f0d2be35a890deb89639a2f4cfb79e0d
8d680895b357c42688ed53ee8d2df001
4809fc2bc429444b06ae44420a13434c
f7f789bcd34e88130bb1552190569ed5
f065d8eee8f4343540177c38dabafd0a
60770a887f5384ca4b157ed57ce7ba55
c3c6c12d7f9fa4681a9fa64209b94c00
3be83f3c8ea052a1e6f6d9d1bb9641c3
bad9703a337e63e2680d7f6e5eb49445
d580991d2caa2bea3d406941f44cc32d
00f206b3dfc921f0c696b0c346e39fc9
06807d8d7282959ce062f92a708d382f
c665fa0aa5afa3fb41c21afe5884b4f1

Remediation

To reduce exposure to Pay2Key.I2P and similar ransomware threats, organizations should implement the following:

- **Block script execution** (.cmd, .ps1) from user-writable paths.
- **Disable 7-Zip SFX and restrict unknown archive execution**.
- **Audit Defender exclusions** and remove unauthorized entries.
- **Deploy EDR/XDR** to detect behavioral anomalies (PowerShell abuse, scheduled tasks, DACL changes).
- **Apply system and software updates** regularly.
- **Enforce MFA** and limit administrative privileges.
- **Monitor. i2p traffic** and block darknet-related endpoints.
- **Train employees** on phishing and ransomware risks.
- **Ensure secure, offline backups** and test recovery procedures.
- **Maintain a ransomware-specific IR plan**.

ThreatCure

Cyber Threat Advisory

Secure your byte world

Pay2Key.I2P

Ransomware-as-a-Service (RaaS) Campaign