Chaos Ransomware Variant Sides with Russia

⋮ 5/18/2022

Since the beginning of the ongoing Russia-Ukraine War, some ransomware and hacking groups have publicly declared which side they are on. Such actions have created tension internally within the threat actor groups as it has caused dissension, and externally, as organizations fear being targeted due to the political nature of the war.

One notable example is the Conti RaaS (Ransomware-as-a-Service) that officially announced in February 2022 that they are backing Russia and would use their arsenal against critical infrastructures that belong to the West. Fear spread quickly as many organizations around the globe had been victimized by the Conti group in the past, with stolen data exposed and critical files being encrypted. However, the Conti group was bitten back soon after the announcement was made. An allegedly unhappy Conti insider took the matter in their hands and leaked Conti's internal chat logs to the public.

On the other side of the debate, the LockBit ransomware group made it clear that they will not involve themselves in the political war because of the multinational nature of its developers and affiliates.

In this vein, FortiGuard Labs recently came across a variant of the Chaos ransomware that appears to side with Russia. This blog explains the vicious consequences that the Chaos variant delivers to a compromised machine.

Affected Platforms: Windows
Impacted Parties: Windows users
Impact: Potential loss of files
Severity Level: Medium

Technical Details

A GUI-based Chaos ransomware builder is known to be available that can easily customize the malware according to a set of options. FortiGuard Labs recently discovered a sample of malware that seems to have been created using this builder. Unfortunately, how the malware arrives on a victim's machine is unknown. However, given the political stance of the malware (the blog will cover this later), the malware likely arrives either via forum posts or emails focused on the current Russia-Ukraine war.

Once the malware runs, it enumerates the files on all drives. For files smaller than 2,117,152 bytes, it generates a random 20-character long password for each file and then encrypts it with AES-256 (CBC-SALTED). Each encrypted file contains an RSA encrypted password with a hardcoded public key + base64 encoded AES encrypted file content. The malware also adds a 'fuckazov' file extension to the affected files. Figure 1 shows the content of an encrypted file. "azov" may be a reference to the Azov Battalion who put up a fierce fight against Russian military forces in the Azovstal steel plant in Mariupol, Ukraine.

README.txt.f[redacted]kazov:

```
<EncryptedKey>eewHsnD5Q1msKhcDRpY9GQu39mERKORNXiyKmn+BCGAlAQgQGS7AIKuQb1HygkQUIPQlV4iu
Kq6GD3XDikV9Q5Ugb3OxyrnYs7Pv+2xe2ab10Mkf2kNeBWflF9LRM2E/mB3eBlhfKNHYAGBACTS+45xHloCpwv
4ObKer7XuqkoA=<EncryptedKey>5odpv1fUnaE/iCYWnSyaf7DC4CNSg/iLYO7UiEEAc6AGR9rA8T1mprle/O
xxS0rO0a4v5boMmwLy9Jo/7XXlV84QyMJkjR4HIyWq6/Bfd/PrLVykEJy+cf9pAWKMh57aANR0LtINs3zc5bxO
AqHdF8J+ZVxKfP+dZkrFttN3tuHu95sfuwX8ZTQH2Nr6JHRP2cxLzDGbV43sBdScpMOMQN1XlkXwkPGemEQQIm
xEe/YaAFviJKxxUiTqsy0AOCP6CD2cLeaH3tUY54gEc7xgY1ji52SBQkTeYjeWnZj5RGs3Mfq31Nm/CFvpJWM3
89pGlDtQcjNEJj5a7ARe8E8nYWIoeSWZgj0gXLjqgYoafL4YFfn8PAciu1JarMNEd0dLhSmnicVMx+Iv4TPPkn
2IsZ59JAi3tXF4/6rJqxlTCUenygRewu+c1j94sz+sAHork2f13enm5nrF7YrwVCZRruc05X/rcKjBPVnCxVZK
ZyR/lvrnXYicoAri849rdOEo9VN+ll76KOy14SS+sowYcNppzz4ul+WiWLFz5oPhKvt2+VQM9fEIrXgTuRqTS8
29vTgpVrWEko+GVwvHPXsMZMsPS49eT/jLwNdAHTjMnBrjc2seDwyGDxPMeqCCRZ61thVqB4PFqStXkD4LaZ0V
SCOQBedXLdxYubn8aGFuvfKQvno1Rnd98Tqp1DUnDp1quCc2hVD3Q4wrKNR5qTHbvNZYpbRsQaKy3AOoMHkP0N
0fewQwxce6Mt53QojGBS/UfEmaFkKaDHUyZdXrHaRIKMpXa/O6cgEKiNCNGGjMQq6uN6sqrEvhsEx4oaIwhIID
AT1G4pu3haGdkoTH1dbuY4bo5JTgLexE93dY71DGATDRIzhJjdzhrgLItbWfsoTSoAzJ+1FwzbI32ve1V3m5c/
jrB2xcYN+mc3b2F81siooW1a/NlyYnMgFUvw3k8HLr+90k7/QnZCPte9DmE9YQZdeJLWPzCdtpSymfpJDFJaRZ
G5D2M7a0ZQkO2NhzSgWqTX+q2Ud5hMZl0/h9bNumGeoFbBsJGcLYmthWBOrsNpZR30dC2HGy2tPSho6OF2wvLl
nkglpCwNLot/yKFpsOH5zwzAfvVVfqqWNnqkZkEi83XcvE6bEmObjskr7T20QhNg2nwovPUBLyOy8p7OnNtAaH
r8tIb+Swgr466q+0SlI4ww7C6QBSXduKg5vXZ+Yit3ctQOsRa+gWlRqe5Y/Aq/qDASjnMxrfOFj373MYYCI1Wp
UrabE9R4VpiF2Bnx2sirzBjhS43umpdCkZrE1PO59S6996oGmjNnoL+0ibC+LxbQr091zXwXOP5m7KpaOh/J2U
9W2yLwBSSZfV9uLgr7wskT8U5nr3gj8vMz24xe4z7H/fQ/yO2EhOvjR9+I1WbxFtymgTX3pPTiiGkvmwVIr4ME
I7wLPfSJY/5qpJ37hmcuISRCRiqtdJSeMqFwB92My5z8RV7yyvaShmmFQSZrPG0ROwhf5n4oNaiJYmExGYPoZt
r4wKGEiF/ZwzS2g4pr6IfH6Mf5Y3XJsNgO9yHbXJfYSUDuOauxr9yv7MKnHMCCm7blAOrslK7FDPMr8fIkAXDV
+a3EF9lAjqG/UiVE78k/piCwK6uqeY9mmiLjCvRDIPxf2gdgLDfFf88eBcOUT+fFv1c0gB+A8NTTeusFu7WGeb
pX3UvYQdw2r66mIGW9OAK42AwUfujoH2yMiuAvwDjt4Y9ifzK7ZHCRuz5yQm8K+x8kWM78IIkOrbYmF8lBn5FJ
Cp0S4R/tfQkgepji1OGYWYR6cB/E5AhDCgAQwFFbKT/nXi4f6NtYTnPhb4BGVf5c1yl0s8LoF31QCkZfQjfcq9
SqhwfxeW+fAaxeZXPPTsg2npauCYZxVfRUZ8gVme/SsDRQNQ8dQYGWQLbE4B4fOJ+Jh+Q56n8lrpASBsy4ubgp
lfyRQXkCVlD6DmNCfoih+WJ3JR3ydMGhxyXkeUwiO7rvJLf+IH38v4cXr+ogHqVt+8hmolQ2n+N1zN0QGoOL8E
1QZmUe1vGmjIMwQ6v4BurDafodgbWXMa1KJ9ZLSTgyUjwHHl/LMcu9wnI6/dXC6eOY/cKHdF6OGl
```

```
Brown: RSA encrypted random PASSWORD
Green: AES encrypted file content, where AES key is derived from PASSWORD
```

Figure 1. Content of an encrypted file

For files larger than 2,117,152 bytes, the malware fills them with random bytes, making file recovery impossible without backup. The affected files also have 'fuckazov' as a file extension.

For the C: drive, the malware searches for files in the following directories and either encrypts or fills them with random data depending on the file size and adds a 'fuckazov' file extension.

"\\Desktop"; "\\Links"; "\\Contacts"; "\\Desktop"; "\\Documents"; "\\Downloads"; "\\Pictures"; "\\Music"; "\\OneDrive"; "\\Saved Games"; "\\Favorites"; "\\Searches"; \\Videos.

Its malware activities are typical of recent Chaos ransomware variants. Like most ransomware, it displays a message in "stop_propaganda.txt". However, things get a bit interesting from here as it displays the following message:

*Stop Ukraine War! F**k Zelensky! Dont go die for f**king clown!*
You can see the truth here:
t.me/[removed]
[removed].ru

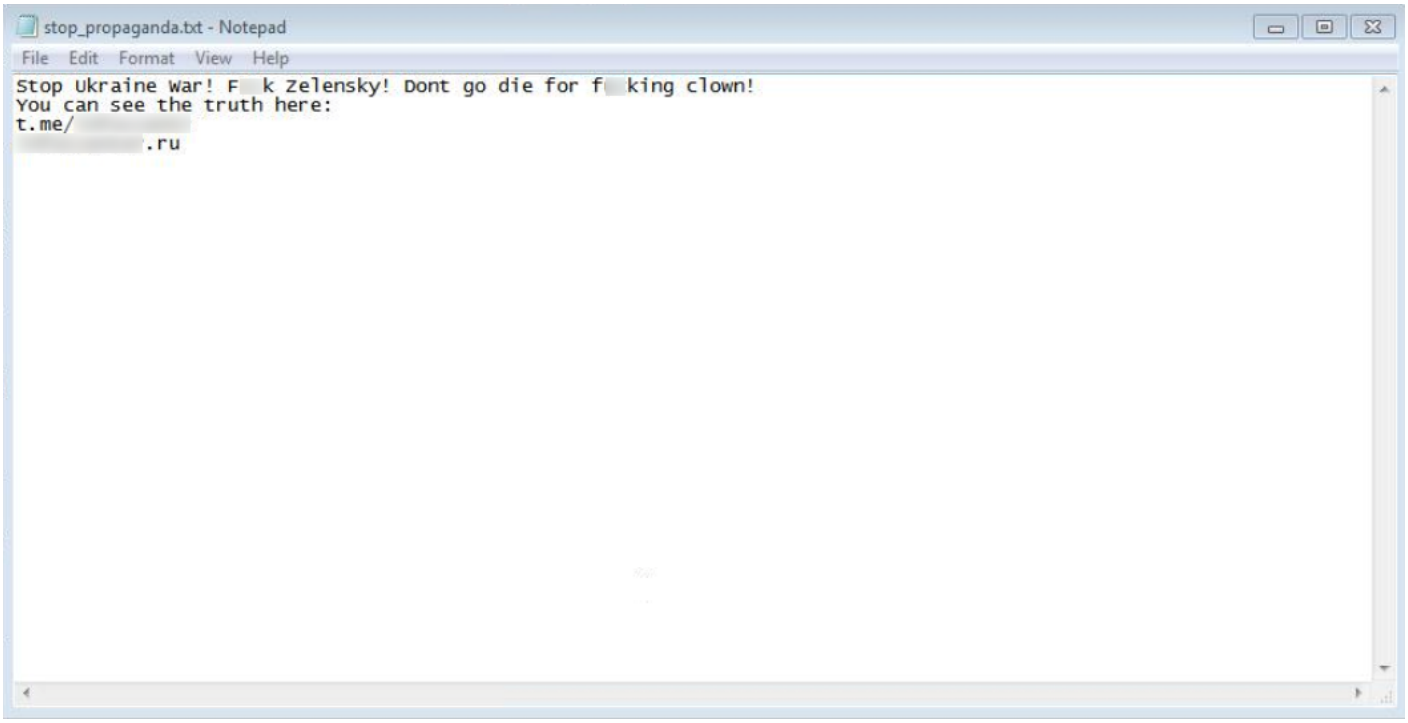

Figure 2. Message displayed by the malware

As seen in Figure 2, there is no ransom demand nor any information on how the victim can reach out to the attacker. The links on the message leads to a Russian Web page, created in April 2022, with what appears to be political messages and information:

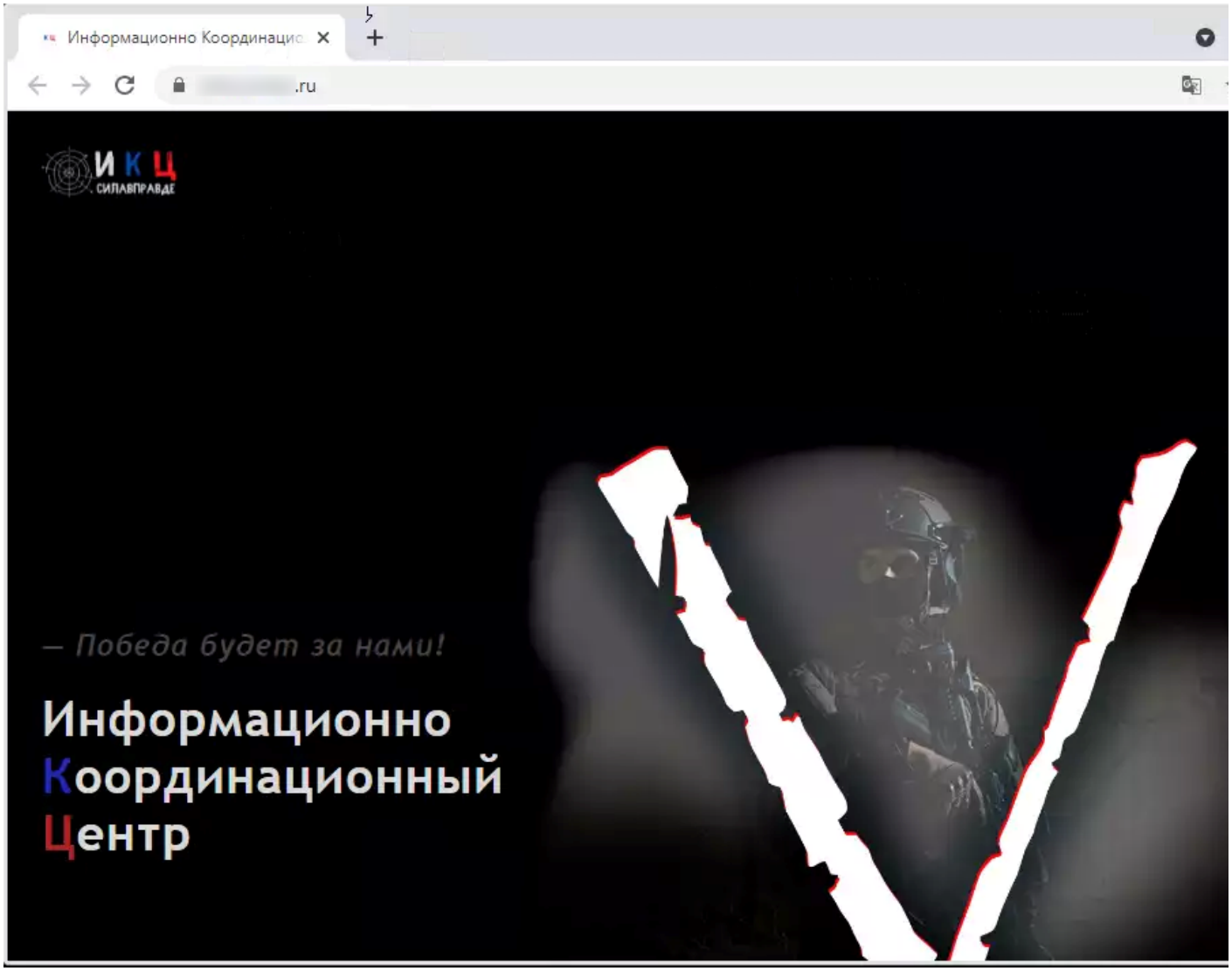

Figure 3. Screenshot of the Web page linked in the message displayed by the malware

The message reads in English:

“- Victory will be ours!

Information and Coordination Center”

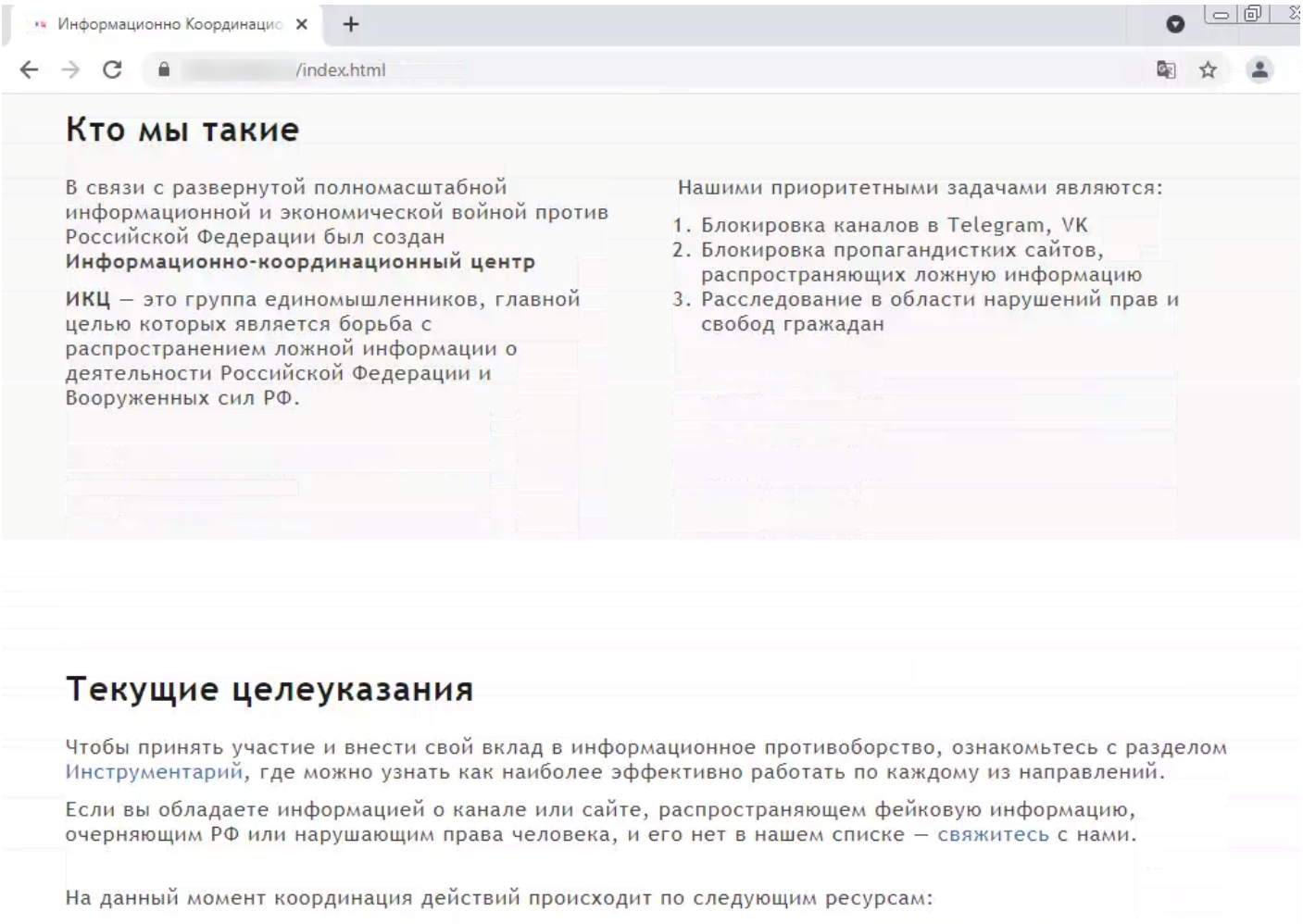

Figure 4. Description of the Web site

Machine translation into English is as follows:

Who we are

Our priorities are:

In connection with the full-scale information and economic war unfolding against the Russian Federation, the Information Coordination Center ikts was created - a group of like-minded people whose main goal is to combat the spread of false information about the activities of the Russian Federation and the Russian Armed Forces.

1. Blocking channels on Telegram, VK 2. Blocking propaganda sites,

2. Blocking propaganda sites that disseminate false information

3. Investigating violations of rights and civil rights and freedoms

Current Targeting Guidelines

In order to participate and contribute to the information confrontation, please see the Toolkit section, where you can learn how to work most effectively in each area.

If you know of a fake news channel or website which is spreading false information, defaming Russia, or violating human rights and it is not on our list, please contact us.

At the moment the following resources are being coordinated:

The Web site also appears to include a list of Ukrainian soldiers who were either killed in combat or who are considered war criminals in the eyes of the Russian Armed Forces.

While typical Chaos ransomware variants provide at least some hope to the victim that files smaller than 2,117,152 bytes that were encrypted might be recovered upon ransom payment, this particular variant provides no such avenue as the attacker has no intent on providing a decryption tool. Combining that with the deletion of shadow copies from the compromised machine, which inhibits file recovery, makes it awfully difficult for non-tech savvy victims to recover their affected files.

The malware appears to be fresh as it was likely compiled on May 16th, 2022, for this attack.

Conclusion

The Chaos ransomware variant that this blog covers is unique in the sense that the attacker has no intention of providing a decryption tool or file recovery instructions for its victims to recover their affected files. Finding them is a tall order for non-technical victims, which pretty much makes the malware a file destroyer. Clearly, the motive behind this malware is "destruction." The politically inclined messages also indicate that the attacker is pro-Russian and frustrated with the current situation. And with the Chaos ransomware builder now readily available, its options allow anyone to create destructive malware. And with no end to the war in sight, FortiGuard Labs expects more malware like this to emerge.

Victims of ransomware are cautioned against paying ransoms by such organizations as CISA, NCSC, the FBI, and HHS. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities which could potentially be illegal according to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory.

Past Chaos Ransomware Analysis

You can read more about the Chaos ransomware in the following FortiGuard Labs publications:

- Chaos Ransomware Variant in Fake Minecraft Alt List Brings Destruction to Japanese Gamers
- Fake Windows 11 Upgrade Assistant Program Leads to Destructive File Encrypter

Fortinet Protections

FortiGuard Labs has AV coverage in place for the malicious file sample in this report as:

MSIL/Filecoder.AGP!tr.ransom

Fortinet customers are also protected from this malware through FortiGuard's Web Filtering, FortiMail, FortiClient, FortiEDR, and CDR (content disarm and reconstruction) services.

Due to the ease of disruption, damage to daily operations, potential impact to the reputation of an organization, and the unwanted destruction or release of personally identifiable information (PII), etc., it is important to keep all AV and IPS signatures up to date.

In addition to these protections, Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

We also suggest that organizations have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats that is designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

MITRE TTPs

Collection	
Data from Local System	T1005
Credential Access	
Credential in Files	T1552.001
Defense Evasion	
File Deletion	T1070.004
Discovery	
System Information Discovery	T1082
Execution	
Command-Line Interface	T1059
Impact	
Inhibit System Recovery	T1490

IOCs

File IOCs

954d8fcd6b74d76999f9ec033ca855ffdab6595be23039f03bc4c6017fa3932c