HabitsRAT Used to Target Linux and Windows Servers

By Joakim Kennedy

Published: 2021-04-20 · Archived: 2026-04-05 19:05:51 UTC

We have discovered a new malware written in Go, which we are calling HabitsRAT, targeting both Windows and Linux machines. The Windows version of the malware was first reported on by Brian Krebs and The Shadowserver Foundation in attacks against Microsoft Exchange servers. In addition to this version, we have identified a newer Windows variant and a variant targeting Linux environments. As of this writing, the Linux version is undetected by all Antivirus engines on VirusTotal. We assess that the Linux version is used to target Linux servers in an adjacent campaign to the one reported by The Shadowserver Foundation. The malware allows the attacker to control the compromised machine remotely. To protect themself from being taken over by others, the attacker's commands are signed by a private key that only the attacker has access to. The malware does not execute commands that are not signed by the correct key, suggesting that the malware has been developed by a sophisticated programmer.

Intro

On March 28th, Brian Krebs published a blog post about attacks against Microsoft Exchange servers. In one of those attacks, a webshell called "**Babydraco**" was deployed. The webshell was used to deploy a new malware. The binary had the filename "**krebsonsecurity.exe**" and used a Command and Control (C2) server located at "**brian[.]krebsonsecurity[.]top**". This malware turns out to be a remote access trojan (RAT) that has been written to target both Windows and Linux machines. Based on strings found in the malware, we have named it HabitsRAT.

While the Windows version of the RAT has been documented being installed on compromised Microsoft Exchange servers, it is not known what type of servers the Linux version is used against. Still, in the last couple of months, numerous remote code execution (RCE) vulnerabilities have been disclosed in hardware and services running on top of Linux. About a month ago, CISA released an advisory urging users of F5 BIG-IP to apply patches to address RCE vulnerabilities.

Technical Analysis

The HabitsRAT is a simple backdoor that allows the malware operator to execute arbitrary code on the infected machine. While the backdoor is simple in design, the malware has functionality making the attack more complex than what is normally seen. The malware is written in Go and targets at least both Windows and Linux machines. The structure for the Windows version of the malware, generated by redress, is shown in the code snippet below. Most of the code is shared between the Windows version and the Linux version. The operating system-specific code has been placed in the files "**commandplatform_windows.go**", "**keyplatform_windows.go**" and "**persistencehandler_windows.go**". The rest of the files are shared with the Linux version.

Package main: C:/Users/user/habits/habits-client

File: commandhandler.go

RunSignedCommand Lines: 17 to 35 (18)

File: commandplatform_windows.go

RunCommand Lines: 8 to 13 (5)

File: keyhandler.go

GetOrGenerateKey Lines: 13 to 23 (10)

GenerateKey Lines: 23 to 42 (19)

GetKeyStore Lines: 42 to 50 (8)

SetKey Lines: 50 to 68 (18)

GetKey Lines: 68 to 77 (9)

File: keyplatform_windows.go

GetRootKeyStore Lines: 11 to 19 (8)

GetUserKeyStore Lines: 19 to 27 (8)

IsRoot Lines: 27 to 49 (22)

File: main.go

main Lines: 17 to 34 (17)

File: persistencehandler.go

InstallPersistence Lines: 9 to 17 (8)

CopyBinary Lines: 17 to 22 (5)

File: persistencehandler_windows.go

CheckPersistence Lines: 11 to 21 (10)

GetBinStoreRoot Lines: 21 to 29 (8)

GetBinStoreUser Lines: 29 to 37 (8)

InstallPersistRoot Lines: 37 to 98 (61)

The Linux source code structure is shown in the code snippet below. The Linux specific code has been placed in the files “**commandplatform_linux.go**”, “**keyplatform_linux.go**” and “**persistencehandler_systemd_linux.go**”.

Package main: C:/Users/user/habits/habits-client

File: commandhandler.go

RunSignedCommand Lines: 17 to 35 (18)

File: commandplatform_linux.go

RunCommand Lines: 8 to 13 (5)

File: keyhandler.go

GetOrGenerateKey Lines: 13 to 23 (10)

GenerateKey Lines: 23 to 46 (23)

GetKeyStore Lines: 46 to 54 (8)

SetKey Lines: 54 to 72 (18)

GetKey Lines: 72 to 84 (12)

IsRootAsString Lines: 84 to 86 (2)

File: keyplatform_linux.go

GetRootKeyStore Lines: 9 to 16 (7)

GetUserKeyStore Lines: 16 to 17 (1)

File: main.go

main Lines: 17 to 34 (17)

File: persistencehandler.go

InstallPersistence Lines: 9 to 17 (8)

CopyBinary Lines: 17 to 20 (3)

File: persistencehandler_systemd_linux.go

Systemd_CheckPersistence Lines: 11 to 25 (14)

Systemd_GetBinStoreUser Lines: 25 to 33 (8)

Systemd_InstallPersistRoot Lines: 33 to 64 (31)

Installation

When the binary is run, it installs itself into a folder. The Windows version's location is "**%SystemDrive%WindowsDefenderMsMpEng.exe**" while the Linux version is "**$HOME/.config/polkitd/polkitd**". This will result in the malware being installed under "**/root**" if it's being run with root privileges.

After the malware has installed itself, it checks if the persistence method has been set up. If it hasn't, it goes ahead and sets it up. On Linux, it uses a "systemd" unit file. The malware checks if it's already configured by executing the command "**systemctl status polkitd**", as shown in Figure 1.

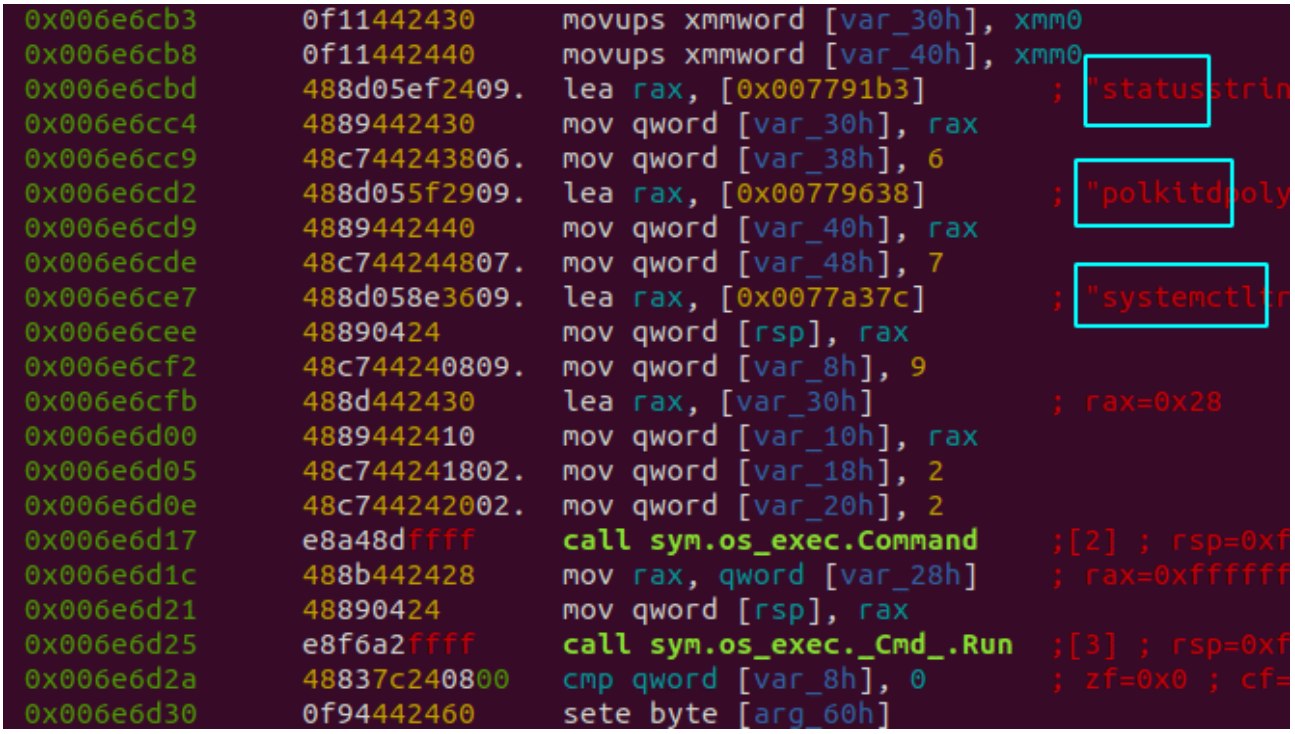

Figure 1: Linux version of the malware checks if persistence has been configured already.

The systemd unit file is created at "**/etc/systemd/system/polkitd.service**" and its content is shown in the code snippet below.

[Unit]

Description=Authorization Manager

After=network.target

[Service]

GuessMainPID=no

ExecStart="/path/to/binary"

Restart=always

[Install]

WantedBy=multi-user.target

The Windows version of HabitsRAT uses scheduled tasks for persistence. First, it writes the scheduled task "**xml**" to a file located at "**%TEMP%krebsonsecurity.xml**". The content of the file is shown in the snippet below. The task is added by executing the shell command: "**sCHtAsks.exe /create /xml %TEMP%krebsonsecurity.xml /tn WindowsDefenderScan**"

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2"
xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2020-12-18T09:56:46.3915265</Date>
    <Author>Microsoft Corporation</Author>
    <URI>\Microsoft\MicrosoftUpdater</URI>
  </RegistrationInfo>
  <Triggers>
    <BootTrigger>
    <Enabled>true</Enabled>
    <Delay>PT1M</Delay>
    </BootTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
    <UserId>S-1-5-18</UserId>
    <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
```

```
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
<AllowHardTerminate>false</AllowHardTerminate>
<StartWhenAvailable>true</StartWhenAvailable>
<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
<IdleSettings>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
<AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context=”Author”>
<Exec>
<Command>
pathtobinary
</Command>
</Exec>
</Actions>
</Task>
```

Command and Control Communication

The RAT uses public-key cryptography to both encrypt and authenticate the commands from the C2 server. The malware generates a public-private key pair using an open-source library provided by Proton Mail. Figure 2 shows the call to the GenerateKey function and its arguments. The malware uses the machine's hostname as the name and an email address of "**a@a.a**". No password is provided and it's requesting a 2048-bit RSA key to be used.

The key is stored and written to disk. The Linux version of HabitsRAT writes to "**$HOME/.config/.accounts-daemon/accounts-daemon.login.conf**" if it is running as a normal user or to "**/usr/share/accounts-daemon/accounts-daemon.so**". The Windows version uses "**%SystemDrive%WindowsDefenderMsMpEng.dll**" or "**%APPDATA%Windows NTDefenderMsMpEng.dll**" instead.

Figure 2: Generation of public-private key pair using the open-source library from Proton Mail.

HabitsRAT sends a "check-in" *POST* request to the C2 server to see if it should execute a command. As part of the request, it sends some data about the infected machine. The form data of the request is shown below. The data includes the "**no_replay**" field that holds the sha256 hash of some random data. This acts like a nonce to prevent executing the same request multiple times. The request also includes the public key for the malware instance. This is to allow the C2 server to encrypt the commands to it. It also has a version value that is hardcoded to 11.

no_replay: [sha256 hash of random data]

public_key: public key in ascii armour

hostname: [machine hostname]

goos: [linux or window]

goarch: amd64

shell: [$SHELL expanded]

root: [true or false]

version: 11

The data is sent to "**https://brian.krebsonsecurity[.]top/checkin**". If no command is returned, the malware sleeps for 10 seconds and sends the request again. If the C2 responds with data, the malware checks that the threat actor's key has signed it. A hardcoded public key is included in the binary. Extracted information from the key shows that it was generated in December 2020 and includes a name and a Gmail address.

pub rsa3072 2020-12-03 [SC] [expires: 2022-12-03]

uid [REDACTED] <[REDACTED]@gmail.com>

sub rsa3072 2020-12-03 [E] [expires: 2022-12-03]

If the correct key has signed the response, HabitsRAT uses its private key to decrypt the payload. The data has been serialized to JSON and the malware unmarshals it to the data structure shown below.

```
type main.CommandList struct {
    No_replay string
    Commands []string
}
```

The Commands field is passed as arguments to either "**bash -c**" for the Linux version or "**cmd /c**" for the Windows version.

HabitsRAT Version 12

A newer Windows version of HabitsRAT has also been found. Much of the functionality is the same as version 11. The main difference is that it's using a different C2 public key and supports multiple C2 addresses. As can be seen from the snippet below, this key was generated on the 2nd of April.

pub rsa3072 2021-04-02 [SC] [expires: 2023-04-02]

uid Brian Krebs <krebsonsecurity@gmail.com>

sub rsa3072 2021-04-02 [E] [expires: 2023-04-02]

The malware uses four different C2 addresses and picks one out of random. The addresses are as follows, which includes a domain of Brian Krebs's leaked social security number:

- https://brian-krebs-erectile-dysfunction[.]com
- https://krebsonfellatio[.]net
- http://XXX-XX-XXXX.com (Redacted)
- hxxp://185.193.126.198

The addresses are stored at:

- %SystemDrive%WindowsDefenderDefender.dll
- %APPDATA%Windows NTDefenderDefender.dll

Conclusion

The HabitsRAT is a multi-operating system malware targeting both Windows and Linux environments. There is a lot of code reuse between the two variants. It provides the attacker with the capability to execute arbitrary code on the infected machine. To protect its C2 communication, the data is encrypted and signed using PGP. Ensure internet facing servers are patched to prevent being infected by HabitsRAT. Indicators of Compromise (IoCs) below can be used to detect if a server has been compromised. Go malware has been hard to detect by Antivirus products so it's likely this trend will continue. We have seen threat actors pivot and target different operating systems with the same codebase for the malware, resulting in low or undetected malware samples, especially for Linux—which has a large presence in the cloud. Since the malware is derived from the same codebase, detection based on code reuse has proven to be very effective.

Runtime protection with Intezer Protect gives you immediate visibility over all code running in your systems and alerts you whenever unauthorized or malicious code is executed. Intezer Protect users can detect and mitigate threats like HabitsRAT on their Linux systems. Protect 10 hosts for free with our community edition.

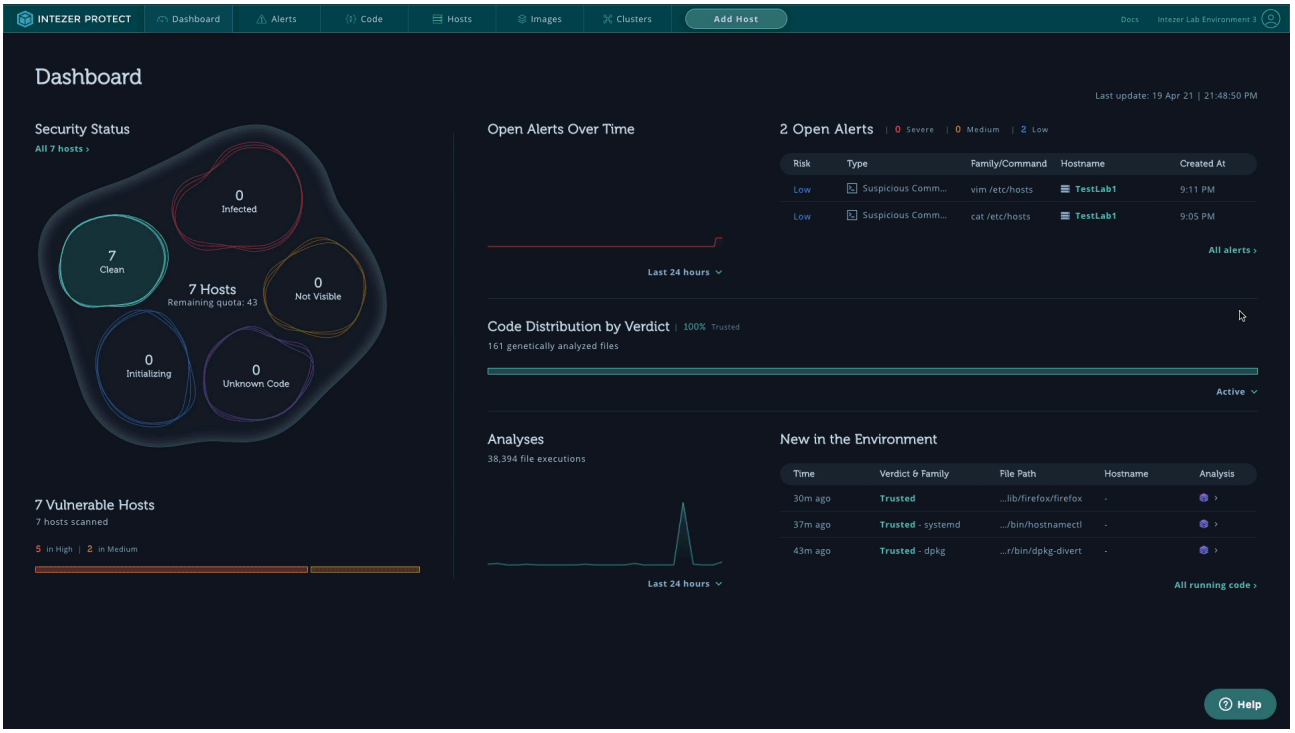

Figure 3: HabitsRAT detection in Intezer Protect.

IoCs

Hashes

Windows version of HabitsRAT

- 29ebf9771e52cde90776eeccd89aaf4c19577ef136258daef1a17c767ce88c9d
- 37a16e79e5be132d7e6c2e1ee482d80d93ad942af7110a4bc3a05f0b575236b0
- 5f7d898ade3162bfb0c8d3006c42e934ff81fab3b4ad3b51c13441fd63e438cb

- 9e840be4b4ab358bc3405e2c688f3ab1a9d286bd4fb9edb4468dc688962b4893
- f556c9b4e5bb463be84dead45a9aedcf8bec41c1c2b503ea52719357943750e7

Linux version of HabitsRAT

- 338e41f1a8be56339b039835b06d815a3666c8b0d5725b63be7bf54c8745704a

File paths

- %SystemDrive%WindowsDefenderMsMpEng.exe
- $HOME/.config/polkitd/polkitd
- /etc/systemd/system/polkitd.service
- %TEMP%krebsonsecurity.xml
- $HOME/.config/.accounts-daemon/accounts-daemon.login.conf
- /usr/share/accounts-daemon/accounts-daemon.so
- %SystemDrive%WindowsDefenderMsMpEng.dll
- %APPDATA%Windows NTDefenderMsMpEng.dll
- %SystemDrive%WindowsDefenderDefender.dll
- %APPDATA%Windows NTDefenderDefender.dll

Network indicators

- brian[.]krebsonsecurity[.]top
- brian-krebs-erectile-dysfunction[.]com
- krebsonfellatio[.]net
- 185.193.126.198

C2 public keys

Version 11

—–BEGIN PGP PUBLIC KEY BLOCK—–

mQGNBF/I9bUBDACtHQlddPduY2DXMrQHxsh+jCP2ojeMi+08VmuC/eCG3+x0815p

ymssBejVcCckahu0EIJZIl5WaRY+nOJKF9VOdLoegpVmqPmX3GE0FJBR/cGGLSqQ

bofuDbWBIwQPVwHT+QriDpAK9M80H5f6FPm2HqcXJV2fI7FJ5pLWSTMRGhnTjt5D

aSiZqbXhYuq1W3S4zWSsh0TZPn0a4J44N/MwrlrPtr+Q+p31diEHPhQVQZ7a6QKD

ysM3SAx5hSUueli6nawRt6UkOhTbeL1SaGA1dv3PHliTLvOt+OZ6oEAU8aKp3Y2S

PQ3jKkR7x6jzkRNbu3DoXz70Te97f5ZS0qS6WFWSnpTXWC8JN0NG0cG3tDZ9ClyH

NhNnMKl040y33BzBzhQmQmHaX7NwwqEB54HIYsfE4fiSrKovxOkBBXcmS8sPhuhH

Hk6ZiXqEzlB+pIMvtXvNWT3qqhOC/ggmCUpt1YNHnOYoI93A+dlpbRSbmFOkSwL0
Zvd3RhzddtTIUf8AEQEAAbQnTWF0dCBIYXluaWUgPHBhemVyZnJvbXNpbHZlckBn
bWFpbC5jb20+iQHUBBMBCAA+FiEEmgXO4h7loKvki421YmZthezMP4EFAl/I9bUC
GwMFCQPCtQsFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQYmZthezMP4Ex/gv9
FHhkSKm9u5REhdCF+Ez8jk4LzoLGOaNdA8hcMCVHBWCMeE3yTGHec1P16WAqJhG+
LmlfpS7r0QIANeZC2W0rFI2b/lMBFzpzynR2Fi/Gpph4chNlzqlQJWgSvlBPsw0M
nnNwpzRfQhbcSdS/j+zFPE01bSkpm93TczcIvXvdFqJQfpU03pHrAFAvA1pmBkEW
NOmZ8JgLn+HReJQCeCteUbiBdGVIDPneyENZzRcO3fuXzlg3yysPIFKRBbGAqiCt
gtf+RsoyQ19k5vTSjXHK1KYWVvE9dA4levuN8iYKLhPxpBDNGSkY0n5NqECQpkJW
oG0dTDzMDtbAAdjhsoFIv4vH3aGr3iuoYv1ax5WxBSRb2h4Zno0Np4emo91p8FS4
KQXuNivYO5SXcEiXNRfDbUSN3J51b6v+SZGmdDhQUEWrEQ7MGl8eBT7DH3+ioZtO
qtezE/MnDzRIZW+o7yeryF9/aqLCa5oEFKNKgHM6n9Jmh4KAip1oiJArCJUHUQkI
uQGNBF/I9bUBDADrDvqlvnPjMQNXCWdlKjBgmiVAcWxRe5NmdIe4d43GdLXEOsWI
eTNY1/L5g4ZLXTeTgMo9ugU9bhwviWq6gro2hPXZVmBhHEVEAtICNjFTlHBOUhab
U+riCEeNzE3jneqfS/x04eNirM7hAplSOMOtag49TPwjzqnqGr1r/oe8L1BXHcUP
Cl6EQzk4NSGrNVO8E7Ppm7yeDnK9C0+4LXaMu19np/r43lg1FBk6O4d/q4/S7p+q
P/TILTDC0hPSQw+aAjQPKlfWAjZUQ0CcJT1A5x5SIVWqlpL85ltphdJzCmCiTtmm
kMIvX86OxZkzhligkJ1r1QM8OL+t9Mzq9mglc6PHUXIISiaVvwI3ZWH1OxI6ate3
znV8n3wfAbURDoTmPCMSNziSrvT39zsUCxY7zQoKoeNUBmx8AWW0Sgms2z1oK8ti
+JekSBbxLNVElglwDgtSLkgA4dOnfTUtCDstZouxVnenhLD7jUSmhbS+XIkjsOUY
+mXshXvqEb1rD5cAEQEAAYkBvAQYAQgAJhYhBJoFzuIe5aCr5IuNtWJmbYXszD+B
BQJfyPW1AhsMBQkDwrULAAoJEGJmbYXszD+BbzUMAIviQCxye0jQVnHwT1JjnyjF
7JaiJlU2nOQave16DmyHcu0rejJLhJoQXaA28Qgkv+6mOK4fXWyPV+iAcr3AKuTV
EVY6EDwwUwGn/RxcIYVt8qSZanj+cd6g9iJR3UMb9//25ggIW618NvW0zODowwNu
GDF5ei4cyhvA3NjCCqIvwxO+XRJynp+0lQl0ulOCS+Y+/V3H0+0EhIrJ8x5TvnE9
yC8CtagR0S53mNtmbS3A8INV/Gj6M7/7BZ2eVkbZRVEoQkhmr/lvJ/n4QhYcgre9

1iboJ75TorVEOH1B0Q/3IACBD/fEnSogjij8Vf/bdb4W/8LHpeV8bbtDzkzMfh7i

SxoF8y1kBl/YXrbs4mFcwgQ8KKqKkYkMp9p527LF/gglE54xMMXdp2WG65oh5jZz

0vzASRgwAI+K0LuN1+McUJwWtWQlcnQEEDlvbHVe1jKOrdqqf+BRxl2rNDU0P+u+

mtrn7vMinEja8k6O2N2RsL0TvLyGD+sAPKUZG7Q/Bg==

=gbms

—–END PGP PUBLIC KEY BLOCK—–

Version 12

—–BEGIN PGP PUBLIC KEY BLOCK—–

mQGNBGBm0jYBDAC83QCJbnqPtHUfazjzNEeNmHY2zUeV8tXaKUkFyeIG9QmSSZ4u

0Y+uNR3p5CkexQC0C6STIkDE43fYU92N+Olt7jFcYK718vPv6ieGSuuztJqnrOKX

9jY/22iRPYFNjcw+LPQzm4CXyD3gugfp3Jm1JO99y5D5PDbP6yVpG6Fm6TmzOXku

grLoWBLWBn5Z6BJAB1YYM35vJpjC22eY6uFF6fhAW7K8mZNUKYHGwZOfkK5F+27Y

lxiaOHjh0mjfisWWvcvlImd5dd7614Pu5Yl3PfH4p7fUZJsGofj+hyiZHd9luIM1

yc9TWSQBSeBKIFM9iU7a4i0vB4rbY355tYBckuCVyt4NNBnDO0/zgVOZkf/qjTm+

JUZlxQJ54Gs7aWueo/aWSaqCN/TIqD909coDbw+sUA1CojLsw+ghPJBBzB/sSjzA

OCvGOVn+TCr8hV8OBpONXRQFUO4do6VALE/tqBlMMy12Lq/DunM87Mrb9zpJGZyh

JkqGP05xdT9omIEAEQEAAbQnQnJpYW4gS3JlYnMgPGtyZWJzb25zZWN1cml0eUBn

bWFpbC5jb20+iQHUBBMBCgA+FiEEOQFTY4snpri84X9c/wQVl3dsa2QFAmBm0jYC

GwMFCQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ/wQVl3dsa2QgEQv+

Px8Vl1WxzlWWoZsAkmLsXZzPuudAAFWai97g89/D3+D8kxKAiqq2mam9YKx/Cimn

B4HwGhE7ildWfVcJUx63t30Vm8rMIg1M63PQJ+CSIIU8cNEsWSOr8RIcfCTcenDZ

ZdK761c1xNXypag/oToTdDTOCRlfeLFkw2fgcHVsxJoIH00MtAT1utqo7xl15kGk

0jodlv6mDp17E4JBcg2aT4HpzVUIgeDOzCi5b8QPj0X1iDes8DolYu1wHnNaVAXg

SNshR5v5VbrFXvKfyx7sRA8lxQn4HkmnOH18drG+gsE0msFoveqf2M5BCzItY2bI

wG+GQwUTAwciIh5AehbpKOqrk2m588PI11i0x8bc5z3/I3YZbWhdpyJAmNErE/Et

X5nSqVn2lDoooDA9AwE6fRr2oNNxDLE0yREt88cD2EE3/iweQbpeGBSneIFKGdW3

b8zQdJi30gAe7kVS3FFnYXqNaHNhKm/WvODzwRNLSAN6Z1KwJZ79Q3uh19vkl6vr

uQGNBGBm0jYBDACxBNtcNethMzVIig0BIQbrCJ4wVS01waB3WWe71s9RUbJn/LFd

pey/f0NQrMdoUJP75Do91cS6SFI956F7l5AMWAWTDrNkiCQTG8ptegdAJQ81qWAd

V0L2YH+8CNYmfmTOqh3L+cOya6yanNMMM1+c1zjQjCLWzOZog7tBm+1891Gwy8nT

m1jf+oETqUcVV+ePrGaaNLWOB+U69/q6XOScaV/HeQrYLE6MTsoiFgKNEirrDDzj

rd3bjFZzttD8Cuknt7rsOtZC393JHMSu4f2SPy2Wct1r77z2PxBIkKjTJS3Ax2Lf

3rZ3Yt08v1Bmjyxq+zXoIUuSwSNnAP7AJyBKaOtZ/BRjT4xYL9uf0LaIC/a840SB

B3f9N3YzfYgL6GeRib6vv6OrWRPjs/ld8kaj1/l6m2Ry+VIs/433AWMp6b0nQqnS

EMy/72RuSxQogRbgNnwjk6mIBpEyeTQ7mXHslxK5fJVAOPdOGIVAQziQ82BdA9Yw

92ha17TJ1nKz/x8AEQEAAYkBvAQYAQoAJhYhBDkBU2OLJ6a4vOF/XP8EFZd3bGtk

BQJgZtI2AhsMBQkDwmcAAAoJEP8EFZd3bGtkCZAL/ioNDjl54jiVARfIdqSZPS77

tkkB+dGSuJgeZ+60/1gDpGXaWEyx73Mfbp+DT80k2JQ86Cls9S5xuy95gECMo/JI

Jxc5gPdXEH+II+wmfVbQerf1cPmjlSliaRDczJKdO5R14i7IEnD56c+MYDqBvTvH

NAyjFqPrVXBUcqiuDva8PvUN+dcLGBYwGemlNHCt0L7kQ6TPjldjqSjyeUragJYO

Ak4lz+E4cl+V5xKWjFw81S2+sHVLUNmR4KaY5iyfSBSDgNDFW5xQrnClJBg0+4cv

QqDJRd4JJOYjBp/dLjmGeXmxuVyshGePUBYrOCsm1GTf3Razr+lgpn4OzW78MRVv

JFfcpGhafyTvZQrV7qa7Na8fjSLr+drbDDxm3WP2Tz9Un0tuDvayLhTU/AnWY2MT

v+LlwbUDmdrZx+VwMCj4ZwtYkVSqHUd1yfZ5s6I+yPcN6700Kw0dea628GEC+g9V

QE+GLOcciRHTBgzaL16trl40wZQ8iMpgnn/FEz+grw==

=6v1j

—–END PGP PUBLIC KEY BLOCK—–

Source: https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers