Internet of Termites

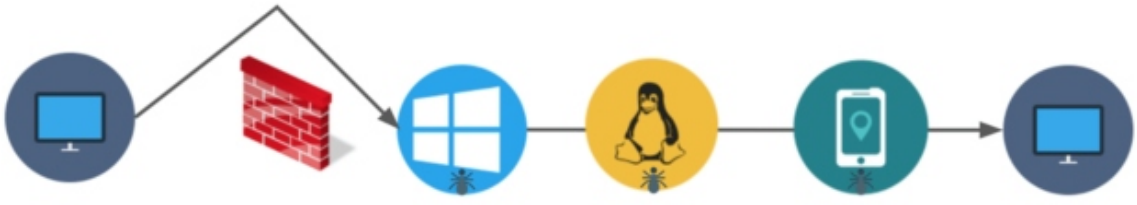
alienvault.com/blogs/labs-research/internet-of-termites

1. AT&T Cybersecurity
2. Blog

March 6, 2019 | Chris Doman

Termite is a tool used to connect together chains of machines on a network. You can run Termite on a surprising number of platforms including mobile devices, routers, servers and desktops.

That means it can be used used to bounce a connection between multiple machines, to maintain a connection that otherwise wouldn't be possible:



Termite is a useful networking and penetration testing tool, but we're seeing it used in attacks to enable access to machines too. There has been little reporting on Termite, beyond a brief mention in a report by Kaspersky of an earlier version of Termite called "EarthWorm". Below, we've provided an outline on some of the attackers we're seeing deploying Termite.

Note: As we were publishing this, Symantec released a report on attackers using Termite in the 2018 attack stealing the health data of a quarter of the Singapore population.

How Termite and EarthWorm Work

Termite and EarthWorm are publicly available tools written by an employee of 360NetLab. They can be considered an updated version of the well known packet relay tool HTRAN.

Termite popped up on our radar when we were reviewing malicious binaries compiled to run on IoT architectures. Termite is available for a range https://github.com/rootkiter/Binary-files/tree/master/Termite/release/agent of different operating systems and architectures including x86 ARM, PowerPC, Motorola, SPARC and Renesas.

This means an attacker can use a long chain of desktop, mobile and IoT devices to be able to connect through networks and DMZs.

Termite can act as a SOCKS proxy to bounce traffic, as well as a lightweight backdoor that can upload and download files, and execute shell commands:

```
*************************************************************************
                    A)  BASE COMMAND
 ---------------------------------------------------------------------
0. help                             This help text.
1. show                             Display agent map.
=========================================================================
                    B)  AGENT CONTROL
 ---------------------------------------------------------------------
1. goto     [id]                    Select id as target agent.
2. listen   [port]                  Listen Mode  (on target agent).
3. connect  [ip] [port]             Connect Mode (on target agent).
=========================================================================
C)  START A SERVER ON TARGET AGENT, AND BIND IT WITH LOCAL PORT
 ---------------------------------------------------------------------
1. socks    [lport]                 Start a socks server.
2. lcxtran  [lport] [rhost] [rport] Build a tunnel to remote host.
3. backtran [rport] [lhost] [lport] Build a tunnel from remote agent.
4. shell    [lport]                 Start a shell server.
5. upfile   [from_file] [to_file]   Upload file from local host.
6. downfile [from_file] [to_file]   Download file from target agent.
*************************************************************************
```

The Termite help function

For example, this is a typical sequence of commands you may see when investigating a compromised machine:

Victim Host	Attacker Host
On a victim host, the attacker listens for incoming connections: agent.exe -l 8888	Then the attacker connects to the compromised machine: admin.exe -c [target_ip] -p 8888 And selects which compromised system to interact with: goto 1 Then they start a SOCKS proxy on the system to route traffic through it: socks 1080 And a shell on the compromised system that they can connect to with netcat: shell 6666

Termite uses a distinctive binary protocol to initiate connections, as can be seen in this network traffic stream:

Network traffic generated by Termite

There is a good description of the command line arguments of EarthWorm here, and the source code of the agent is on GitHub.

Malware

Mobile EarthWorm used to Spy on Targets in Taiwan

We were surprised to find EarthWorm also packed into malware - presumably to provide packet relay functionality.

In one Android application, EarthWorm is hidden inside an image file called box_07.png. The Application communicates with the hostname apache2013.qpoe[.]com - which resolves to a server in Taiwan.

We've previously investigated this server when it was hosting Android malware known as Xsser. The Xsser malware communicates with a familiar hostname apache2012.epac[.]to and impersonates an application from a Taiwanese travel service:

The same server has also previously been associated associated with a group known as “BlackTech” that primarily targets Taiwan.

Windows EarthWorm

We’ve also seen EarthWorm packed in with malware from crypto-mining campaigns.

This malware is linked to a campaign previously reported on by TenCent. Machines at a University Hospital in Guangzhou China, and a children's hospital in Chongqing China, were infected with crypto-mining malware.

Will Cross-Platform Malware Become a Thing?

Network operators report that a significant amount of malicious traffic on their networks are now driven by IoT malware. So far this has been driven by IoT and Linux specific malware such as Mirai and Xor DDoS.

Detection

We detect network traffic across the various Windows, Linux, OSX, mobile and IoT platforms with:

AV TROJAN EarthWorm/Termite IoT Agent Reporting Infection

Additionally our host agent detects EarthWorm/Termite activity on hosts, and generically detects shell connections.

OTX Pulse

You can view indicators in OTX.

Yara Rules

```
rule EarthWorm : LinuxMalware

{

   meta:

      author = "AlienVault Labs"

      copyright = "Alienvault Inc. 2019"

      license = "Apache License, Version 2.0"

      sha256 = "f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd"

      description = "EarthWorm Packet Relay Tool"

      strings:

       $elf = {7f 45 4c 46}

       $string_1 = "I_AM_NEW_RC_CMD_SOCK_CLIENT"

       $string_2 = "CONFIRM_YOU_ARE_SOCK_CLIENT"

       $string_3 = "SOCKSv4 Not Support now!"

       $string_4 = "rssocks cmd_socket OK!"

   condition:

      $elf at 0 and 2 of them

}

rule Termite : LinuxMalware

{
```

```
 meta:
    author = "AlienVault Labs"
    copyright = "Alienvault Inc. 2019"
    license = "Apache License, Version 2.0"
    sha256 = "6062754dbe5503d375ad0e61f6b4342654624f471203fe50eb892e0029451416"
    description = "Termite Packet Relay Tool"
    strings:
        $elf = {7f 45 4c 46}
        $string_1 = "File data send OK!"
        $string_2 = "please set the target first"
        $string_3 = "It support various OS or CPU.For example"
        $string_4 = "xxx -l [lport] -n [name]"
condition:
    $elf at 0 and 2 of them
}
```

Suricata Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"AV TROJAN EarthWorm/Termite IoT Agent Reporting Infection"; flow:established,to_server; content:"|00 00 00 01|"; offset:1; depth:4; content:"|00 00 00 01 6b 00 00 00 01|"; distance:7; within:9; content:"agent"; distance:4; within:5; pcre:"/+?[ -]+?+?$/R"; reference:url,https://github.com/anhilo/xiaogongju/tree/422136c014ba6b95ad3a746662be88372eb11b09; classtype:trojan-activity; sid:xxx; rev:1;)
```

EarthWorm and Termite

SHA256 Hash

```
381774ed8d6d69975694247acc80e42831ee68b43583c8734af52adff8f73373

980fd1e947a8dd578c45bc76254b6aaa95b35e6ec33b8f41da268623500bd0f1

3d9aaac0a8e5c7eadd79d8d5c16119d04f4e9db7107fc44a1e32a8746a1ec375

1ae62dbec330695d2eddc7cb9a65d47bad5f45af95e6c8a803f0780e0749a3ad

27cd70b47588aa0a1c8d737cde89fe8de1351af49aa8f11378a1e26a40f268eb
```

3537b3eaad16d59c1f0c22d6cbcfe5a1b4542cc4f6a1e3135e26873c0dd4b06f

459333b4765363526b2f76353941a5e1346e9a71433bd16c1e34a03c3c13bf6b

3141ce911e3da8b0bf9744ef0603f7fac55be157eafc54995a752759882da1b2

18c3accc4f65aae7bf7897adef35abdcca3697884860a6b5360e4f2d07bc26ed

46af7c0674c69df2af1905ea58288f24d2d10e644d5446d8d2b71b251e8e70bd

e05ef2747f973d6ae9e4bd5fbeede55b27afd44882b83b4aee79330e856757e8

a585eb434239e5c1714192482f20ec2483bf8eae4654ef77973524b3a151b455

73fc266095e6d582b79db226145d0990129ad72c584863a61f3bd0e8056a0435

58fcbf640b58a45f2fed22fdd70c5d73ae781274927a2def5f71cb3e4ce02a15

d57cbbc5b6f0d223b5a3470a6a444ea4ef49dad718cbe992c92cca935cfdac7d

ef1d610dd78efae3dfa2eebade2ee76882b7e2b5df140aa068e25519d800bc63

825790dbcdf9b7a69b9a566f71bc167a0a8353e735390c5815b247ac58efa817

da584a49609de5985f5ba64cfb215f0c30c93fac11563ea32afa3820b3327139

a487628dc7647507f77cff66269d5d4588c7647e408b07ec0c4b1f16a93eefc4

8b6d83c919ad123d4b27f3404604e99eeba9196cf81f3210a65d8ae1b89465a6

7aa2f4a66d72adefd632e15dee392cbeab0a843a4890598a9610660897b398f1

afb55dc8b4bcff758082efde93e5ca9c2a6a725b16a4c82e7675393bf46fecfd

d21cccc6cb3f8313098da5b7ad6a37b5349835a702b5caf8e794a7c6903f40c5

5bcac0a74645424d26b217b7725be826b7d558ecbce7ec5d3072d802e1834181

44370c394c70f88cd9ecfb23f9d6570e2134761d1a04deea5205cec31469cfb0

3af0857c9fae7e41683d34af7e04c6ed29439466761512ebbf28bad7561d092b

9b3d82bb1aff3a17a490dd4da09cd315d8e94a52b8caa31ef7a7cf2a89c9d87a

Android Malware

SHA256 Hash

8774f27021146a863accbf34199a378a28ed28a1c616b8741a1dc8021783a4ec

ad560a69ad6aa327b59c123683189dec416889616b652beaa666a5919fe13935

f8478ce363f824fc8dc14cebe84c29a4d12e66536c0250b9f12540e3a511935b

Hostnames

zany.strangled[.]net

apache2012.epac[.]to

apache2013.qpoe[.]com

Cryptomining Malware

SHA256 Hash

b1988efb8f1debd239e0c563f94d22362e43af77284796899f9987622ffb1463

Hostnames

logv586[.]cc

sock5[.]co

Share this with others

Tags: malware, otx, penetration testing, attacks