Stop the Worm

Gitpaste-12

Travis Anderson and Mark Chapman

Table of Contents

This document contains the following resources:

What is Gitpaste-12

Gitpaste-12

- First detected on October 15, 2020
- Used GitHub and Pastebin
- Targets x86 servers
- Targets linux servers and IoT devices

Cyber Kill Chain

Developed by Lockheed Martin

- Intelligence Driven Defense
- Adversary’s
  - Tactics
  - techniques
  - procedures
- APT =
  - Advanced
  - Persistent
  - Threat
- Seven Steps

Cyber Kill Chain

Developed by Lockheed Martin

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

Cyber Kill Chain

#1 Reconnaissance

- Randomly tries IP addresses
- Chooses a random /8 CIDR
  - Example
    i. IP -- 136.36.33.39
    ii. Subnet -- 255.0.0.0
  - Finds available IP addresses

Cyber Kill Chain

#2 Weaponization

- Preplanned and adaptive
- There are 11 already known vulnerabilities this worm will attack depending on the vulnerabilities found.
- When the worm find a port open running tcp, it will attempt a brute-force attack.

Cyber Kill Chain

#3 Delivery

- Downloads script to setup cron job
  - Executes it again each minute
  - pushes updates to the botnet

Cyber Kill Chain

#3 Delivery

- Downloads script from github to strip defenses
  - Firewall rules
  - selinux
  - apparmor
  - Common attack prevention and monitoring software

Cyber Kill Chain

#3 Delivery

- Installs commands that disable cloud security agents
- Intended to target public cloud computing infrastructure
  - Alibaba Cloud
  - Tencent

Cyber Kill Chain

#4 Exploitation

- Intercepts "readir" system calls
- Causes skipping directories in /proc
  - Tcpdump
  - Sudo
  - Openssl

Cyber Kill Chain

#4 Exploitation

- Contains a library call hide.so
  - Loaded as LD_PRELOAD
  - Downloads and executes pastebin files

Cyber Kill Chain

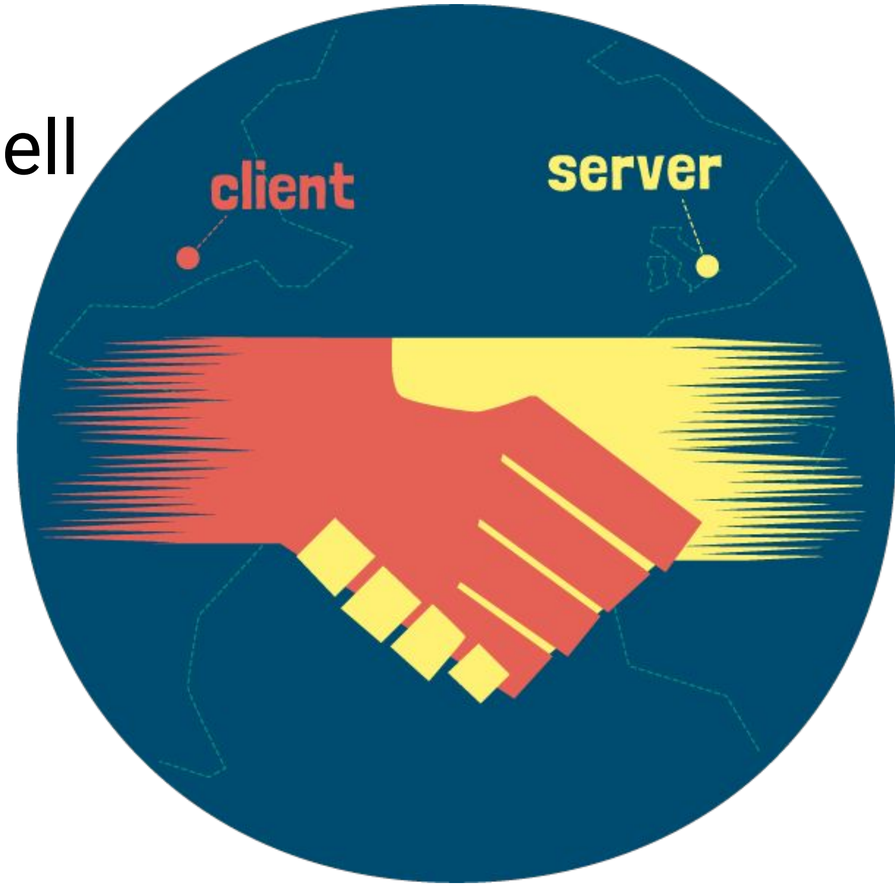
#5 Installation

- Create a botnet
- Monero crypto-miner

Cyber Kill Chain

#6 Command and Control

- Opens ports 30004 and 30005 for reverse shell
- TCP Protocol



Cyber Kill Chain

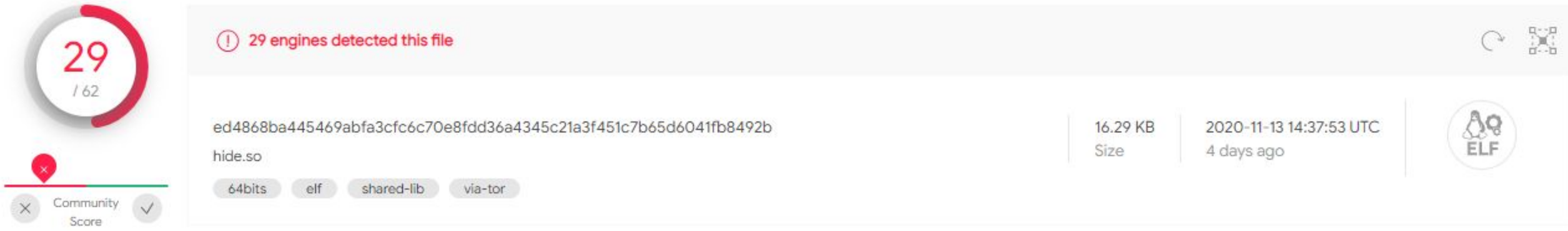
#7 Actions on Objectives

- Monero Crypto Mining
- DDoS

Detection and Mitigation

Detection


4
/ 64
Community Score
4 engines detected this file
ed4868ba445469abfa3cfc6c70e8fdd36a4345c21a3f451c7b65d6041fb8492b
hide.so
64bits
elf
shared-lib
16.29 KB
Size
2020-11-06 06:41:52 UTC
1 hour ago
ELF


29
/ 62
Community Score
29 engines detected this file
ed4868ba445469abfa3cfc6c70e8fdd36a4345c21a3f451c7b65d6041fb8492b
hide.so
64bits
elf
shared-lib
via-tor
16.29 KB
Size
2020-11-13 14:37:53 UTC
4 days ago
ELF

Detection

- Binary analysis
- Behavior-based analysis
- Statistics-based analysis
- Signature-based analysis

Mitigation

```
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
difok = 5
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 12
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
minclass = 4
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
maxrepeat = 2
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
```

```
sysadmin@UbuntuDesktop:~$ sudo chage -l sam
Last password change                                    : Nov 09, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
sysadmin@UbuntuDesktop:~$ sudo chage -M 90 sam
sysadmin@UbuntuDesktop:~$ sudo chage -l sam
Last password change                                    : Nov 09, 2020
Password expires                                        : Feb 07, 2021
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
sysadmin@UbuntuDesktop:~$
```

Mitigation

- Analyze damages
- Remove infected devices from network
- Patch all systems
- Download security updates
- Change system passwords

Vectors of attack

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)

References

References

Alex Burt, T., Madrid, S., & Lands, J. (2020, November 05). Gitpaste-12: A new worming botnet with reverse shell capability spreading via GitHub and Pastebin. Retrieved November 18, 2020, from https://blogs.juniper.net/en-us/threat-research/gitpaste-12

Cisco Security Threat and Vulnerability Intelligence. (2014, November 10). Retrieved November 18, 2020, from https://tools.cisco.com/security/center/resources/worm_mitigation_whitepaper

Kaur, R., & Singh, M. (2014). A Survey on Zero-Day Polymorphic Worm Detection Techniques. *IEEE Communications Surveys & Tutorials, 16*(3), 1520-1549. doi:10.1109/surv.2014.022714.00160

Sharma, A. (2020, November 06). Reverse shell botnet Gitpaste-12 spreads via GitHub and Pastebin. Retrieved November 18, 2020, from https://www.bleepingcomputer.com/news/security/reverse-shell-botnet-gitpaste-12-spreads-via-github-and-pastebin/

Sharma, A. (n.d.). Gitpaste-12: A dozen exploits that silently lived on GitHub, attacked Linux servers. Retrieved November 18, 2020, from https://blog.sonatype.com/gitpaste-12

User, S. (2020, October 08). Zero-day Attacks Detection and Prevention Methods. Retrieved November 18, 2020, from https://www.apriorit.com/dev-blog/450-zero-day-attack-detection

What Is Binary Code & Binary Analysis and How Does It Work? (n.d.). Retrieved November 18, 2020, from https://www.synopsys.com/glossary/what-is-binary-code-binary-analysis.html