2019 5 CERT

Sodinokibi

Sodinokibi 2019 4 26

RDP

GandCrab VPN

Sodinokibi GandCrab

GandCrab

GandCrab

Key Sodinokibi

1360

7

CERT C2

2019 6 13

CVE-2015-1427(ElasticSearch Groovy)

Elaticsearch groovy

networkservice sysguard 3

e sysupdate

go

main.main

systemctI

networkservice

groovy

_search?pretty

http://185.181.10.234/

E5DB0E07C3D7BE80V520/init.sh json

shell sysguard networkservice

sysupdate

init.sh

http://185.181.10.234/ kill

E5DB0E07C3D7BE80V520/init.sh

init.sh Dog

selinux

30

update.sh ssh

iptables

1)

sysupdate

2)

3) CPU

sysguard networkservic

4)

UPX

1) crontab

systemctl stop crontab

rm -rf /etc/cron.d/*

2) crontab

3)

sysguard networkservice sysupdate

4)

5)

config.json

Cvacj Nmu cp Oscpw

Excel

Power Query

Microsoft

木马程序

安天【追影威胁分析系统】无需离析病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

BD YARA

BD

WinXP

Win7 x86)

◆ 概要信息

	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
	BinExecute/Microsoft.EXE[:X86]
大小	290 KB
MD5	FB68A023334313394A9A0CDBFF3717B24
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	

frrnq$--/,//7,/41,4-jji-bcr_gjq,frkj=f_qf;D@46?.011121/172??7?
.AB@DD15/5@02

◆ 运行环境

Win7 x86 6.1.7600 Build 7600	IE9 Google Chrome Firefox Office 2007 Flash WPS FoxitReader Adobe Reader

◆ UDP 信息

IP		IP	
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	137	192.168.122.255	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.111	123	13.70.22.122	123
192.168.122.1	67	192.168.122.111	68

◆ TCP 信息

IP		IP	
192.168.122.[illegible]	49158	23.4.240.82	80
192.168.122.165	49159	192.168.122.155	139

◆进程监控

PID		
2192	target.exe	"c:\a559e68818054feaaf0d733d32019773\share\target.exe"

z z z z z .23/+640/7./6 - ./.+60671501

漏洞“猎杀”

Jim Soudery/文 安天技术公益翻译组/译

0day