AutoIt Used To Spread Malware and Toolsets

- Posted on:May 6, 2013 at 6:59 am
- Posted in:Malware
- Author:
  Kyle Wilhoit (Senior Threat Researcher)

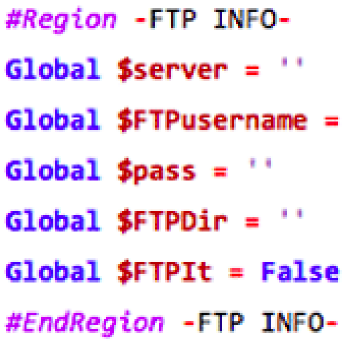
0

18 65 14

AutoIt is a very flexible coding language that’s been used since 1999 by coders looking for a fast, easy, and flexible scripting language in Windows. From simple scripts that change text files to scripts that perform mass downloads with complex GUIs, AutoIt is an easy-to-learn language that allows for quick development. The trend for malicious actors to use AutoIt to code malware and tools however has been increasing, and the trend appears to be getting stronger.

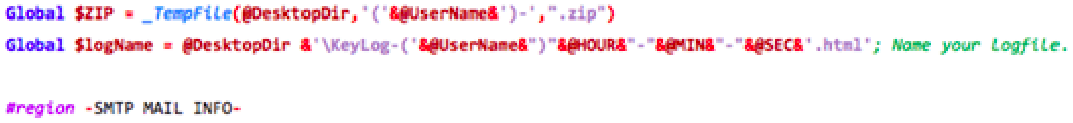
AutoIt Hacker Tools

Recently, we have seen an uptick in the amount of nefarious AutoIt tool code being uploaded to Pastebin. One commonly seen tool, for instance, is a keylogger. Grabbing this code, anyone with bad intentions can quickly compile and run it in a matter of seconds.



```
#Region -FTP INFO-
Global $server = ''
Global $FTPusername = ''
Global $pass = ''
Global $FTPDir = ''
Global $FTPIt = False
#EndRegion -FTP INFO-
```

Figure 1. FTP section of keylogger



```
Global $ZIP = _TempFile(@DesktopDir,'('&@UserName&')-',".zip")
Global $logName = @DesktopDir &'\KeyLog-('&@UserName&")"&@HOUR&"-"&@MIN&"-"&@SEC&'.html'; Name your Logfile.

#region -SMTP MAIL INFO-
```

Figure 2. Sample Code

Upon compiling and executing the script, it creates two files – one that displays the correlated keystrokes in a local HTML page, and a second file that is a zip file of the first file – likely for exfiltration.

In addition to keyloggers, RAT (Remote Access Trojans) builders and server administrators is becoming more prevalent. One RAT builder identified was particularly interesting, as it showed a relatively professional level of development.

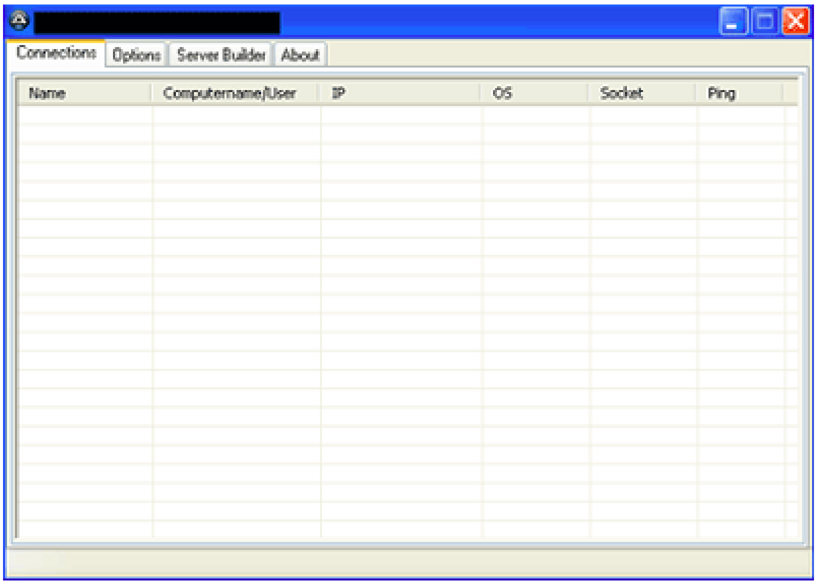

[redacted]

Figure 3. RAT connection tab

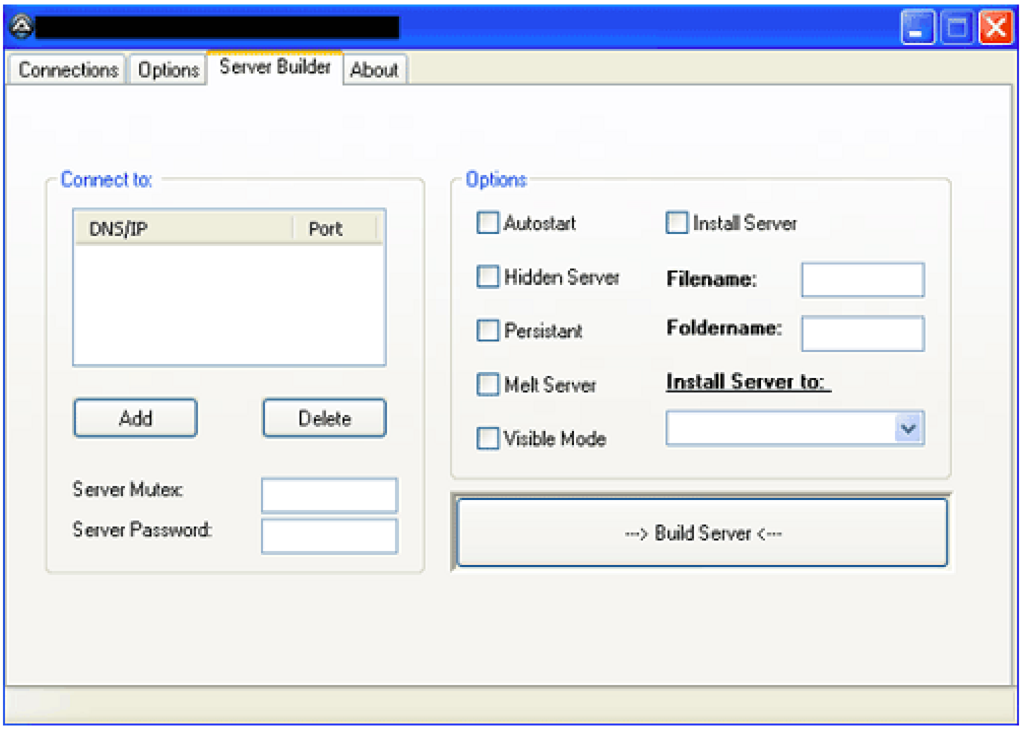
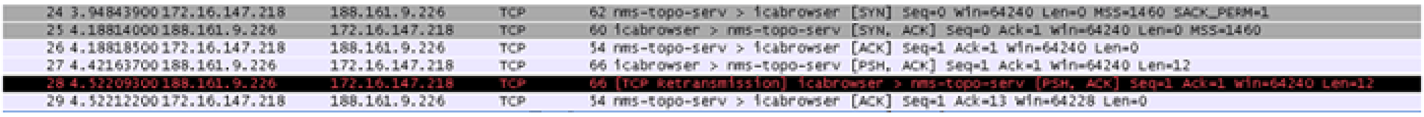


Figure 4. RAT server builder

Upon connecting to this RAT builder/administrator, the nefarious actor can get a remote shell and perform a litany of other system tasks on the victim. Further analysis of this RAT builder traces the developer back to several underground forums.

AutoIt Malware

In addition to tools being found on sites like Pastebin and Pastie, we are also seeing a tremendous increase in the amount of malware utilizing AutoIt as a scripting language. One piece of malware that was found in the wild was particularly interesting. This malware is a variant of the popular DarkComet RAT – utilizing AutoIt. This variant runs a backdoor on the victim machine and communicates outbound to a nefarious host at shark18952012.no-ip.info (188.161.9.226 at the time of writing) over port 1604.



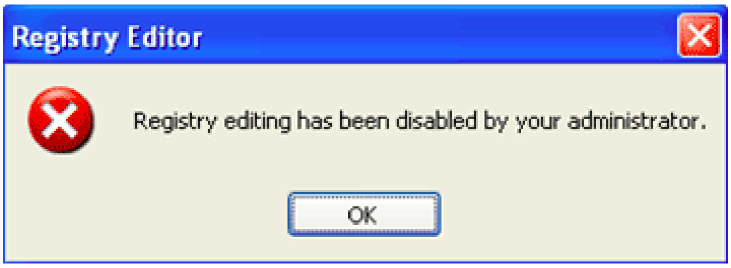
```
24 3.94843900 172.16.147.218   188.161.9.226    TCP   62 nms-topo-serv > icabrowser [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
25 4.18814000 188.161.9.226    172.16.147.218   TCP   60 icabrowser > nms-topo-serv [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
26 4.18818500 172.16.147.218   188.161.9.226    TCP   54 nms-topo-serv > icabrowser [ACK] Seq=1 Ack=1 Win=64240 Len=0
27 4.42163700 188.161.9.226    172.16.147.218   TCP   66 icabrowser > nms-topo-serv [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=12
28 4.52209300 188.161.9.226    172.16.147.218   TCP   66 [TCP Retransmission] icabrowser > nms-topo-serv [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=12
29 4.52212200 172.16.147.218   188.161.9.226    TCP   54 nms-topo-serv > icabrowser [ACK] Seq=1 Ack=13 Win=64228 Len=0
```

Figure 5. RAT communication

In addition to this malware’ s outbound communication, it also modifies the local software firewall policies to disable them, in addition to installing itself at startup for persistency. This variant also drops the following file after execution:

File Name	MD5	File Type
tb2323xt.exe	a53056c5afd30f174af928bd44c05c01	PE File

Upon execution of the malware, it immediately disables the Windows Firewall. After disabling the firewall, the malware then disables the ability to get into the registry of Windows to view or undo the changes performed. Attempting to do so brings up the following error message:



Registry editing has been disabled by your administrator.

Figure 6. Error message

What' s interesting about this malware isn' t that it' s a DarkComet variant, it' s that it is written utilizing AutoIt *and* is detected very sparsely by antivirus products. (Trend Micro detects this malware as TROJ_FYNLOSKI.BU).

Why Do Hackers Like It?

The increased usage of AutoIt is likely attributed to the fact that AutoIt is scalable, very similar to Basic, and is outrageously easy to code in. This ease of use takes the learning curve off learning more complex languages such as Python. This opens up a wide array of possibilities to hackers that may not otherwise expose themselves to a scripting language. In addition, the ability to host code on Pastebin, natively compile, and run applications in stand-alone executable files makes it very quick to develop in. Finally, the ability to natively support UPX packing in AutoIt makes obfuscation easy for AutoIt applications.

Conclusion

As scripting languages like AutoIt continue to gain popularity, we expect more of these types of malware to make a migration to using them. The ease of use and learning, as well as the ability to post code easily to popular dropsites make this a great opportunity for actors with nefarious intentions to propagate their tools and malware. We recommend continuing to update your Anti-Virus signatures as well as consider blocking access to Pastebin, Pastie and other code dropsites on your corporate network where applicable.

We' re trying to make the Security Intelligence Blog better. Please take this survey to tell us how.

Related Posts:

- PwnPOS: Old Undetected PoS Malware Still Causing Havoc
- Steganography and Malware: Final Thoughts
- Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIvy
- DYRE Banking Malware Upsurges; Europe and North America Most Affected

Tags: AutoIT

Featured Stories

- New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths
- Nigerian Cuckoo Miner Campaign Takes Over Legitimate Inboxes, Targets Banks

Recent Posts

- 2016 Predictions: The Fine Line Between Business and Personal
- Pornographic-themed Malware Hits Android Users in China, Taiwan, Japan
- Pawn Storm Targets MH17 Investigation Team
- New Headaches: How The Pawn Storm Zero-Day Evaded Java’ s Click-to-Play Protection
- Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques

Threat Intelligence: The Deep Web

- The latest research and information on the deep web and the cybercriminal underground.
Learn more about the Deep Web

Popular Posts

New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries
Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques
New Headaches: How The Pawn Storm Zero-Day Evaded Java’ s Click-to-Play Protection
Pawn Storm Targets MH17 Investigation Team
Cybercriminals Improve Android Malware Stealth Routines with OBAD

Latest Tweets

Error: Rate limit exceeded

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada

- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies