Operation BugDrop: CyberX Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations

cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

By Phil Neray 2/15/2017

CyberX has discovered a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. Because it eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously "bug" its targets – and uses Dropbox to store exfiltrated data, CyberX has named it "Operation BugDrop."

Operation BugDrop: Targets

CyberX has confirmed at least 70 victims successfully targeted by the operation in a range of sectors including critical infrastructure, media, and scientific research. The operation seeks to capture a range of sensitive information from its targets including audio recordings of conversations, screen shots, documents and passwords. Unlike video recordings, which are often blocked by users simply placing tape over the camera lens, it is virtually impossible to block your computer's microphone without physically accessing and disabling the PC hardware.

Most of the targets are located in the Ukraine, but there are also targets in Russia and a smaller number of targets in Saudi Arabia and Austria. Many targets are located in the self-declared separatist states of Donetsk and Luhansk, which have been classified as terrorist organizations by the Ukrainian government.

Examples of Operation BugDrop targets identified by CyberX so far include:

- A company that designs remote monitoring systems for oil & gas pipeline infrastructures.
- An international organization that monitors human rights, counter-terrorism and cyberattacks on critical infrastructure in the Ukraine.
- An engineering company that designs electrical substations, gas distribution pipelines, and water supply plants.
- A scientific research institute.
- Editors of Ukrainian newspapers.

Operation BugDrop is a well-organized operation that employs sophisticated malware and appears to be backed by an organization with substantial resources. In particular, the operation requires a massive back-end infrastructure to store, decrypt and analyze several GB per day of unstructured data that is being captured from its targets. A large team of human analysts is also required to manually sort through captured data and process it manually and/or with Big Data-like analytics.

Initially, CyberX saw similarities between Operation BugDrop and a previous cyber-surveillance operation discovered by ESET in May 2016 called Operation Groundbait. However, despite some similarities in the Tactics, Techniques, and Procedures (TTPs) used by the hackers in both operations, Operation BugDrop's TTPs are

significantly more sophisticated than those used in the earlier operation. For example, it uses:

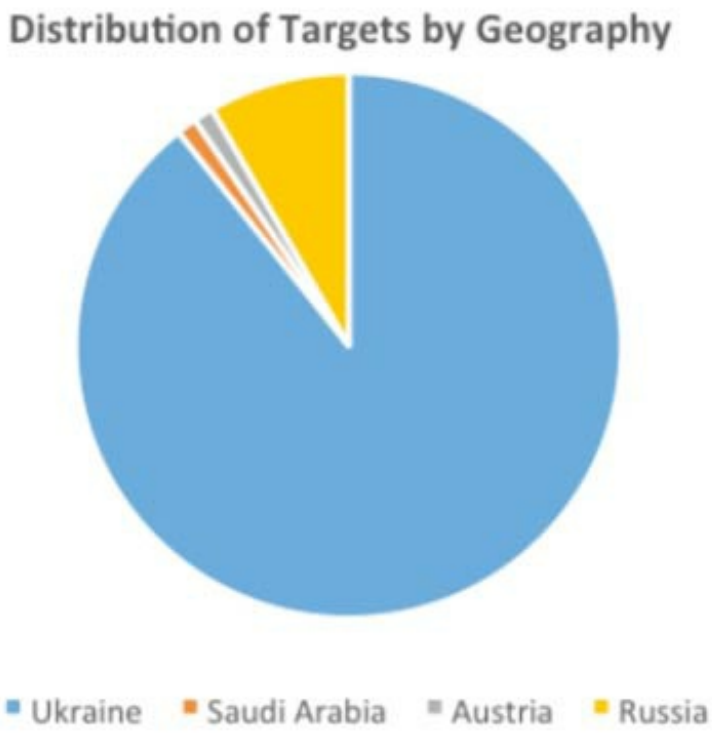
- Dropbox for data exfiltration, a clever approach because Dropbox traffic is typically not blocked or monitored by corporate firewalls.
- Reflective DLL Injection, an advanced technique for injecting malware that was also used by BlackEnergy in the Ukrainian grid attacks and by Duqu in the Stuxnet attacks on Iranian nuclear facilities. Reflective DLL Injection loads malicious code without calling the normal Windows API calls, thereby bypassing security verification of the code before its gets loaded into memory.
- Encrypted DLLs, thereby avoiding detection by common anti-virus and sandboxing systems because they're unable to analyze encrypted files.
- Legitimate free web hosting sites for its command-and-control infrastructure. C&C servers are a potential pitfall for attackers as investigators can often identify attackers using registration details for the C&C server obtained via freely-available tools such as whois and PassiveTotal. Free web hosting sites, on the other hand, require little or no registration information. Operation BugDrop uses a free web hosting site to store the core malware module that gets downloaded to infected victims. In comparison, the Groundbait attackers registered and paid for their own malicious domains and IP addressees.

Operation BugDrop infects its victims using targeted email phishing attacks and malicious macros embedded in Microsoft Office attachments. It also uses clever social engineering to trick users into enabling macros if they aren't already enabled.

How CyberX Investigated Operation BugDrop

CyberX's Threat Intelligence Research team initially discovered Operation BugDrop malware in the wild. The team then reverse-engineered the code to analyze its various components (decoy documents used in phishing attacks, droppers, main module, microphone module, etc.) and how the malware communicates with its C&C servers. The team also needed to reverse-engineer exactly how the malware generates its encryption keys.

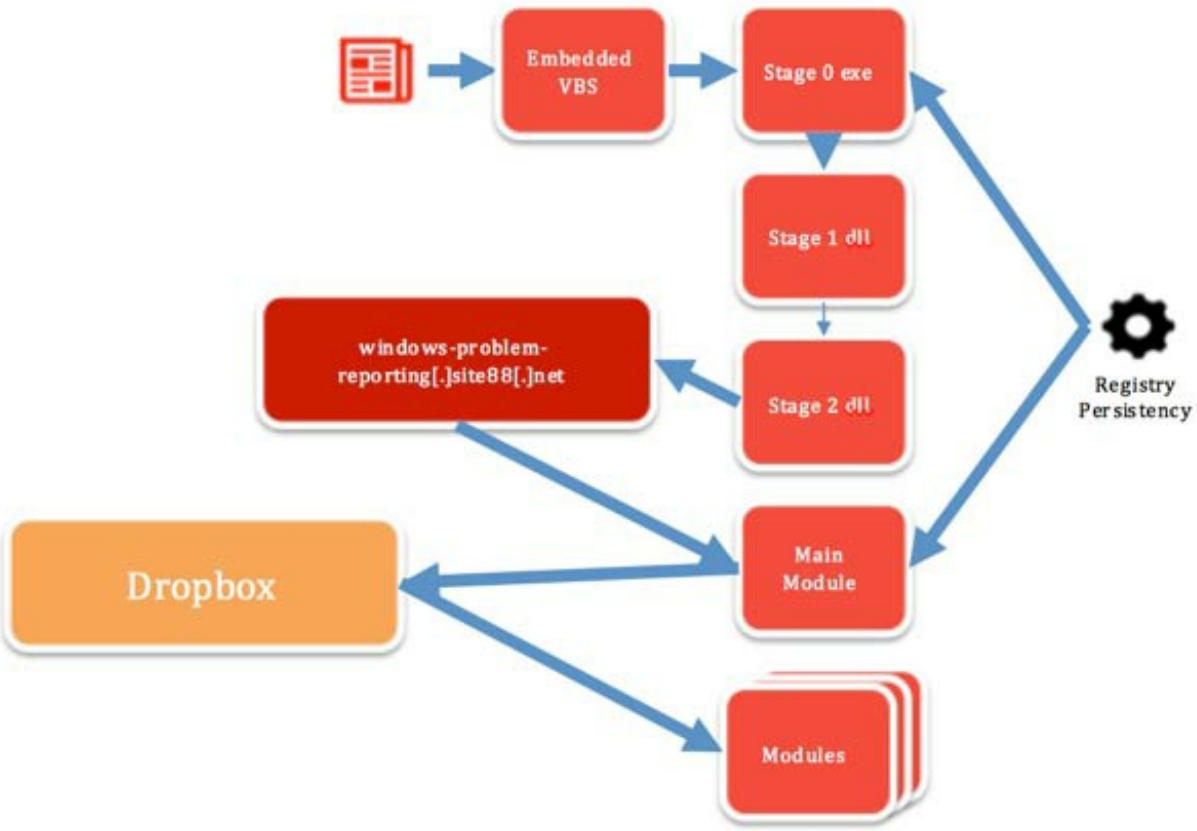
Distribution of Targets by Geography



Compilation Dates

The modules were compiled about a month after ESET announced the existence of Operation Groundbait. If the two operations are indeed related, this might indicate the group decided it needed to change its TTPs to avoid detection.

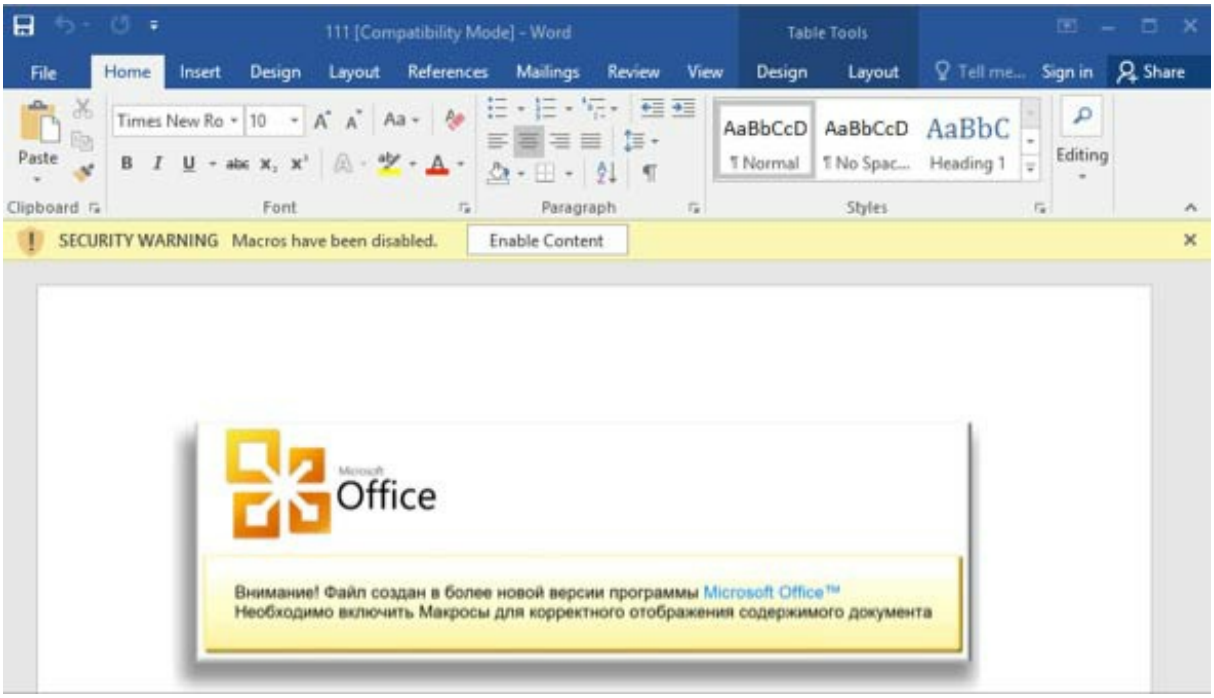
Technical Details



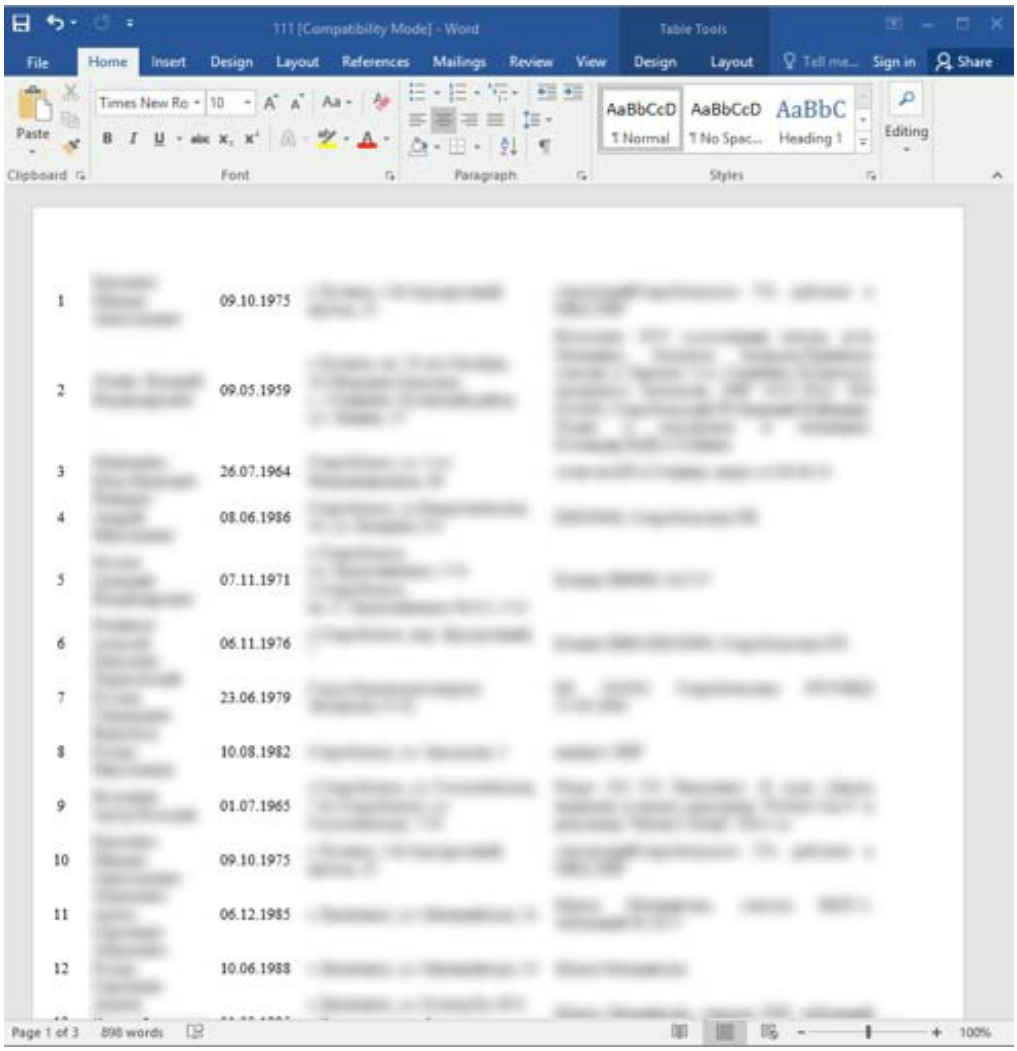
High-level view of malware architecture

1. Infection Method

- Users are targeted via specially crafted phishing emails and prompted to open a Microsoft Word decoy document containing malicious macros.
- If macros are disabled, users are presented with a dialog box (below) prompting them to enable macros. The dialog box is well designed and appears to be an authentic Microsoft Office message.

- 

  - Russian text in dialog box: “внимание! Файл создан в более новой версии программы Микрософт Office. Необходимо включить Макросы для корректного отображения содержимого документа”
  - This is translated as: “Attention! The file was created in a newer version of Microsoft Office programs. You must enable macros to correctly display the contents of a document.”
- Based on the document metadata, the language in which the list is written is Ukrainian, but the original language of the document is Russian.
- The creator of the decoy document creator is named “Siada.”
- Last modified date is 2016-12-22 10:37:00

- The document itself (below) shows a list of military personnel with personal details such as birthdate and address:
    - 

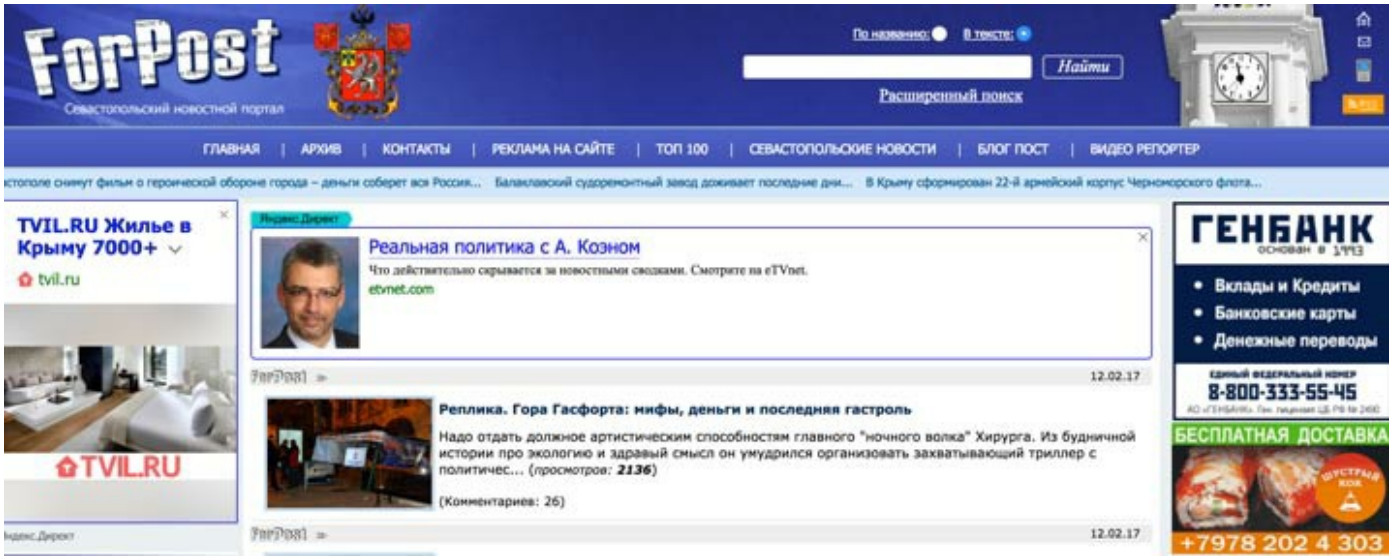
    Decoy document with personal information about military personnel

2. Main Downloader

- The main downloader is extracted from the decoy document via a malicious VB script that runs it from the temp folder.
- The downloader has low detection rates (detected by only 4 out of 54 AV products).

3. Dropper — Stage 0

- The icon for the downloader EXE was copied from a Russian social media site (http://sevastopol.su/world.php?id=90195).
- The icon itself is a meme that jokes about Ukrainians (http://s017.radikal.ru/i424/1609/83/0c3a23de7967.jpg).
- *Dropper icon*



Russian social media site from where icon for dropper EXE was obtained

- The dropper has 2 DLLs stored in its resources; they are XOR'ed in such way that the current byte is XOR'ed with the previous byte.
- This technique is much better than just plain XOR because it results in a byte distribution that doesn't look like a normal Portable Executable (PE) file loader. This helps obfuscate the file so that it will not be detected by anti-virus systems.
- The DLLs are extracted into the app data folder:
  - %USERPROFILE%\AppData\Roaming\Microsoft\VSA\.nlp – Stage 1
  - %USERPROFILE%\AppData\Roaming\Microsoft\Protect\.nlp.hist – Stage 2
- The first stage is executed and the DLL is loaded using Reflective DLL Injection.

4. Dropper – Stage 1 – Achieving Persistency

- Internal name: loadCryptRunner.dll
- Compiled: Mon Dec 12 10:09:15 2016

- Responsible for persistency and executing the downloader DLL, the Stage 1 Dropper registers itself in the registry under the key:
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\drvpath
    - RUNDLL32 “%USERPROFILE%\AppData\Roaming\Microsoft\VSA\klnihw22.nlp”, RUNNER
- The communication DLL is also loaded using Reflective DLL Injection.

5. Dropper – Stage 2 – Downloader for Main Module

- Internal name: esmina.dll
- Compiled: Mon Oct 10 14:47:28 2016
- The main purpose of this DLL is to download the main module
- The main module is hosted on a free web hosting site with the following URL:
    - windows-problem-reporting.site88.net [Note: Do not visit this malicious site.]
- We were unable to find any information about this URL in public data sources.
- Attempting to directly access the URL leads to an “HTTP/1.1 404 Not Found” message.
- It appear as if downloading the module requires manual approval, indicating the need for a human analyst or handler in the loop.
- The main module is then downloaded and loaded into memory using Reflective DLL Injection.

6. Main Module

- The main module downloads the various data-stealing plugins assigned to each victim, and executes them.
- It also collects locally-stored stolen data and uploads it to Dropbox.
- The main module incorporates a number of anti-Reverse Engineering (RE) techniques:
    - Checks if a debugger is present.
    - Checks if process is running in a virtualized environment.
    - Checks if ProcessExplorer is running. ProcessExplorer is used to identify malware hiding inside a legitimate process as

      a DLL, which occurs as a result of DLL injection.
    - Checks to see if WireShark is running. WireShark can be used to identify malicious traffic originating on your computer.
    - It registers itself in the registry under the key:
        - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\hlpAsist
        - RUNDLL32 “%USERPROFILE%\AppData\Roaming\Microsoft\MSDN\iodonk18.dll”, IDLE

7. Dropbox Mechanisms

- There are 3 directories on the server:
  - obx – Contains modules used by the main module
  - ibx – Contains exfiltrated output uploaded by the plugins
  - rbx- Contains basic information about the connected client
- After the stored data is retrieved by the attackers, it is deleted from the Dropbox account.
- The Dropbox user that registered the account has the following details:
  - Name: P*****
  - Email: P********@mail.ru

8. Encryption Mechanisms

- The data-stealing plugins store all their output in: %USERPROFILE%\AppData\Roaming\Media
- Before being sent to Dropbox by the main module, the files are encrypted with Blowfish.
- The Blowfish encryption key is the client ID.

9. Data-Stealing Plugins

- File Collector: Searches for variety of file types that are stored locally or on shared drives (including doc, docx, xls, xlsx, ppt, pptx, pdf, zip, rar, db, txt) . Files are uploaded on-demand.
- USB File Collector: Searches for variety of file types on USB drives (including doc, docx, xls, xlsx, ppt, pptx, pdf, zip, rar, db, txt).
- Browser Data Collector: Used to steal passwords and other sensitive information stored in browsers.
- Microphone: Captures audio conversations.
- Computer Info Collector: Collects data about the client such as Windows OS version, computer name, user name, IP address, MAC address, antivirus software, etc.

Not all of the plugins are downloaded to every target. Each module has a unique extension which is the client ID. This is how the main module knows which modules should be downloaded to a particular target.

Conclusions

1) Operation BugDrop was a cyber-reconnaissance mission; its goal was to gather intelligence about targets in various domains including critical infrastructure, media, and scientific research. We have no evidence that any damage or harm has occurred from this operation, however identifying, locating and performing reconnaissance on targets is usually the first phase of operations with broader objectives.

2) Skilled hackers with substantial financial resources carried out Operation BugDrop. Given the amount of data analysis that needed to be done on daily basis, we believe BugDrop was heavily staffed. Given the sophistication of the code and how well the operation was executed, we have concluded that those carrying it out have previous field experience. While we are comfortable assigning nation-state level capabilities to this operation, we have no forensic evidence that links BugDrop to a specific nation-state or group. “Attribution” is notoriously difficult, with the added difficulty that skilled hackers can easily fake clues or evidence to throw people off their tail.

3) Private and public sector organizations need to continuously monitor their IT and OT networks for anomalous activities indicating they’ve been compromised. Fortunately, new algorithmic technologies like behavioral analytics are now available to rapidly identify unusual or unauthorized activities with minimal false positives, especially when

combined with actionable threat intelligence. Organizations also need deep forensics to identify the scope and impact of a breach, as well as an enterprise-wide incident response plan that can be carried out quickly and at scale.

Appendix
Hashes (SHA-256)

Decoy Document:
997841515222dbfa65d1aea79e9e6a89a0142819eaeec3467c31fa169e57076a

Dropper:
f778ca5942d3b762367be1fd85cf7add557d26794fad187c4511b3318aff5cfd

Plugins

Screenshot Collector:
7d97008b00756905195e9fc008bee7c1b398a940e00b0bd4c56920c875f28bfe
dc21527bd925a7dc95b84167c162747069feb2f4e2c1645661a27e63dff8c326
7e4b2edf01e577599d3a2022866512d7dd9d2da7846b8d3eb8cea7507fb6c92a

Keylogger:
fc391f843b265e60de2f44f108b34e64c358f8362507a8c6e2e4c8c689fcdf67
943daa88fe4b5930cc627f14bf422def6bab6d738a4cafd3196f71f1b7c72539
bbe8394eb3b752741df0b30e1d1487eeda7e94e0223055771311939d27d52f78
6c479da2e2cc296c18f21ddecc787562f600088bd37cc2154c467b0af2621937
01aab8341e1ef1a8305cf458db714a0392016432c192332e1cd9f7479507027f

File Collector
06dcf3dc4eab45c7bd5794aafe4d3f72bb75bcfb36bdbf2ba010a5d108b096dc
daf7d349b1b12d9cf2014384a70d5826ca3be6d05df13f7cb1af5b5f5db68d54
24f56ba4d779b913fefed80127e9243303307728ebec85bdb5a61adc50df9eb6
a65e79bdf971631d2097b18e43af9c25f007ae9c5baaa9bda1c470af20e1347c

USB File Collector:
a47e6fab82ac654332f4e56efcc514cb2b45c5a126b9ffcd2c84a842fb0283a2
07c25eebdbd16f176d0907e656224d6a4091eb000419823f989b387b407bfd29
3c0f18157f30414bcfed7a138066bc25ef44a24c5f1e56abb0e2ab5617a91000

Browser Data Collector:
fb836d9897f3e8b1a59ebc00f59486f4c7aec526a9e83b171fd3e8657aadd1a1
966804ac9bc376bede3e1432e5800dd2188decd22c358e6f913fbaaaa5a6114d
296c738805040b5b02eae3cc2b114c27b4fb73fa58bc877b12927492c038e27c
61244d5f47bb442a32c99c9370b53ff9fc2ecb200494c144e8b55069bc2fa166
cae95953c7c4c8219325074addc9432dee640023d18fa08341bf209a42352d7d
a0400125d98f63feecac6cb4c47ed2e0027bd89c111981ea702f767a6ce2ef75

Microphone:
1f5e663882fa6c96eb6aa952b6fa45542c2151d6a9191c1d5d1deb9e814e5a50
912d54589b28ee822c0442b664b2a9f05055ea445c0ec28f3352b227dc6aa2db
691afe0547bd0ab6c955a8ec93febecc298e78342f78b3dd1c8242948c051de6

Computer Info Collector:
c9bf4443135c080fb81ab79910c9cfb2d36d1027c7bf3e29ee2b194168a463a7

5383e18c66271b210f93bee8cc145b823786637b2b8660bb32475dbe600be46e
d96e5a74da7f9b204f3dfad6d33d2ab29f860f77f5348487f4ef5276f4262311