The Dropping Elephant – aggressive cyber-espionage in the Asian region

securelist.com /blog/research/75328/the-dropping-elephant-actor/

- Kaspersky Lab's Global Research & Analysis Team

Dropping Elephant (also known as “Chinastrats” and “Patchwork“) is a relatively new threat actor that is targeting a variety of high profile diplomatic and economic targets using a custom set of attack tools. Its victims are all involved with China’s foreign relations in some way, and are generally caught through spear-phishing or watering hole attacks.

Overall, the activities of this actor show that low investment and ready-made offensive toolsets can be very effective when combined with high quality social engineering. We have seen more such open source toolset dependency with meterpreter and BeEF, and expect to see this trend continue.

The Attack Method: Infection Vector

Dropping Elephant uses two main infection vectors that share a common, and fairly elaborately maintained, social engineering theme – foreign relations with China.

The first approach involves spear-phishing targets using a document with remote content. As soon as the user opens the document, a “ping” request is sent to the attackers’ server. At this point, the attackers know the user has opened the document and send another spear-phishing email, this time containing an MS Word document with an embedded executable. The Word document usually exploits CVE-2012-0158. Sometimes the attackers send an MS PowerPoint document instead, which exploits CVE-2014-6352.

Once the payload is executed, an UPX packed AutoIT executable is dropped. Upon execution, this downloads additional components from the attackers’ servers. Then the stealing of documents and data begins.

The second approach involves capturing victims through watering hole attacks. The actor created a website that downloads genuine news articles from other websites. If a website visitor wants to view the whole article they would need to download a PowerPoint document. This reveals the rest of the article, but also asks the visitor to download a malicious artifact.

The two main infection vectors are supported by other approaches. Sometimes, the attackers email out links to their watering hole websites. They also maintain Google+, Facebook and twitter accounts to develop relevant SEO and to reach out to wider targets. Occasionally, these links get retweeted, indiscriminately bringing more potential victims to their watering holes.

The Attack Tools

1. Malware Analysis

The backdoor is usually UPX packed but still quite large in size. The reason for this is that most of the file comprises meaningless overlay data, since the file is an automatically generated AutoIT executable with an AutoIT3 script embedded inside. Once started, it downloads additional malware from the C2 and also uploads some basic system information, stealing, among other things, the user’s Google Chrome credentials. The backdoor also pings the C2 server at regular intervals. A good security analyst can spot this while analyzing firewall log files and thereby find out that something suspicious might be going on in the network.

Generally speaking, backdoors download additional malware in the form of encrypted or packed executables/libraries. But, in the case of Dropping Elephant, the backdoor downloads encoded blobs that are then decoded to powershell command line “scripts”. These scripts are run and, in turn download the additional malware.

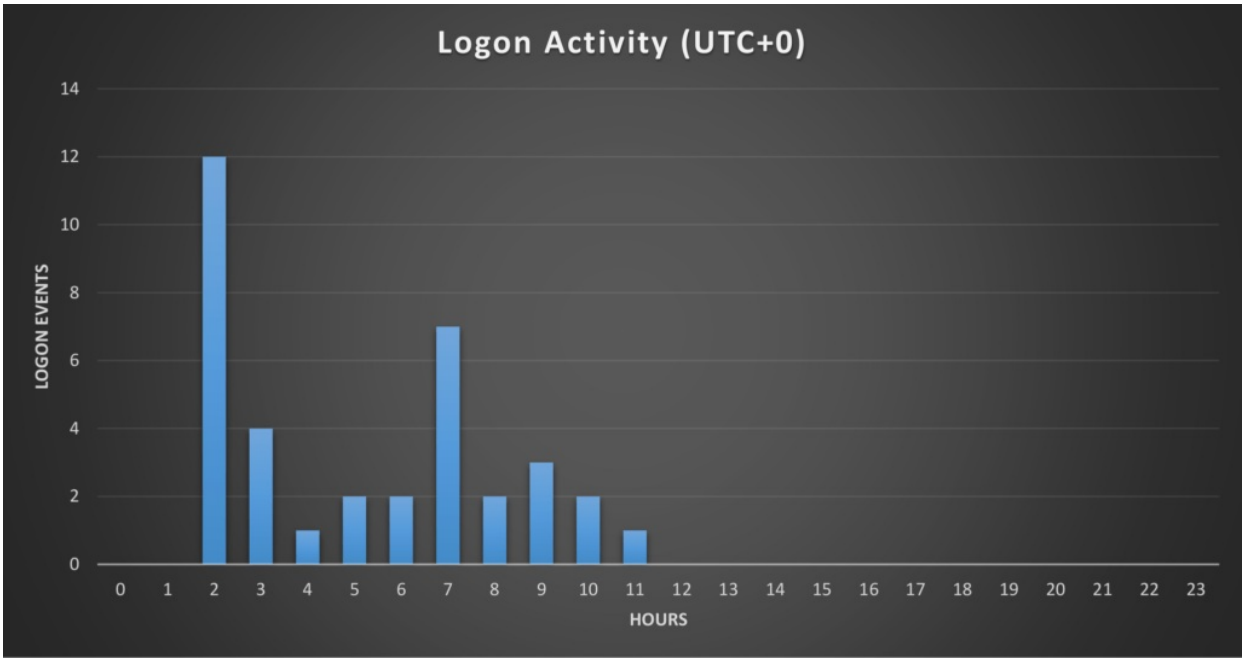
One of the more interesting malware samples downloaded is the file-stealer module. When this file-stealer is executed, it makes another callback to the C2 server, downloading and executing yet another malware sample. It repeatedly attempts to iterate through directories and to collect files with the following extensions: doc, docx, ppt, pptx, pps, ppsx, xls, xlsx, and pdf. These files are then uploaded to the C2 server.

Also interesting are the resilient communications used by this group. Much like the known actors Miniduke or CommentCrew, it hides base64 encoded and encrypted control server locations in comments on legitimate web sites. However, unlike the previous actors, the encrypted data provides information about the next hop, or the true C2 for the backdoor, instead of initial commands.

2. C2 Analysis

In many cases it was very difficult to get a good overview of the campaign and to find out how successful it is. By combining KSN data with partner-provided C2 server data, we were able to obtain a much fuller picture of the incident.

We examined connections and attack logins to this particular C2. As it turned out, the attackers often logged in via a VPN, but sometimes via IPs belonging to an ordinary ISP in India. We then looked at the time the attackers were active, of which you can find an image below.



Victim Profile and Geography

We also wanted to get a better idea of the geolocation of most visitors. Analysis of the image provided access counts and times, along with the IP of the visiting system.

Noteworthy are the many IPs located in China. This focus on China-related foreign relations was apparent from the ongoing social engineering themes that were constant throughout the attacks. The concentration of visits from CN (People’s Republic of China) could be for a variety of reasons – diplomatic staff are visiting these sites from their CN offices, CN academics and analysts are very interested in researching what they believe to be CN-focused think

tanks, or some of the IPs are unknown and not self-identifying as bots or scrapers. Regardless, because we were able to determine that multiple targets are diplomatic and governmental entities, these foreign relations efforts are likely to represent the main interest of the attackers.

Conclusion

Campaigns do not always need to be technically advanced to be successful. In this case, a small group reusing exploit code, some powershell-based malware and mostly social engineering has been able to steal sensitive documents and data from victims since at least November 2015.

Our analysis of the C2 server confirmed the high profile of most victims, mainly based in the Asian region and specially focused on Chinese interests. Actually, some hints suggest the group has been successful enough to have recently expanded its operations, perhaps after proving its effectiveness and the value of the data stolen.

This is quite worrying, especially given the fact that no 0 days or advanced techniques were used against such high profile targets. Simply applying software patches will prevent attacks based on old exploits, as well as training in the most basic social engineering attacks.

However, it should be noted that in this case Microsoft´s patch for exploit CVE-2014-1761 just warns the user not to allow the execution of the suspicious file.

Dropping Elephant artifacts are detected by Kaspersky Lab products as:
Exploit.Win32.CVE-2012-0158.*
Exploit.MSWord.CVE-2014-1761.*
Trojan-Downloader.Win32.Genome.*
HEUR:Trojan.Win32.Generic

As usual Kaspersky Lab actively collaborates with CERTs and LEAs to notify victims and help to mitigate the threat. If you need more information about this actor, please contact *intelreports@kaspersky.com*

More information on how Kaspersky Lab technologies protect against such cyberespionage attacks is available on Kaspersky Business blog.

Indicators of Compromise

Backdoors

eddb8990632b7967d6e98e4dc1bb8c2f
1ec225204857d2eee62c78ee7b69fd9d
d3d3a5de76df7c6786ed9c2850bd8405
05c5cc0e66ad848ec540fcd3af5853b1
0839b3f0a4b28111efc94942436041cb
0cf4acddfaa77bc66c44a687778f8695
233a71ea802af564dd1ab38e62236633
39538c8845bd0b4a96c4b8bc1e5d7ea3
54c49a6768e5f8551d0918e63b200775
7a662144f9d6bada8aea09b579e15562
aa755fc3521954b10fd65c07b423fc56
d8102a24ca00ef3db7d942912765441e
e231583412573ecabfd05c4c0642a8b9
eddb8990632b7967d6e98e4dc1bb8c2f
fb52fbd9b3b465453276f42c46350c25

Exploit documents

d69348794e85ddea6a5f68b85f9bf47b 10_gay_celebs.doc
9f9824e9a4d7d3073aebbcc781869660 1111_v1.doc
d1c864ae8770ae43a0e59a31c0788dc2 13_Five_Year_Plan_2016-20-1.pps
9a0534772ac23ff64e3c85b18fbec596 2015nianshijiexiaoxuanshou.doc
a46d44e227b49d2075730610cfec0b2e 7GeopoliticalConsequencetoAnticipateinAsiainEarly2016_1.doc
79afb3f44172447015578b8064c1dda0 7GeopoliticalConsequencetoAnticipateinAsiainEarly2016_2.doc
6abf60e9e2f6e3fa4c8020e1b2ef2867 ABiggerBolderChinain2016_1.doc
89963d5aac8441b0febbe5d5a0ab7629 ABiggerBolderChinain2016_2.doc
d79e1d6302aabbdf083ba89a7c2f34fc aeropower.pps
90af176bfdf248d2899b49316458e4b6 australia_fonops_1.pps
24c722f3d0770ede82fa3d6b550098b3 australia_fonops_2.pps
08a116efce7d947257ce94fc8f3e276e aviation_1.pps
0ae8f01b9ba0394f5e68536574076aa1 aviation_2.pps
0d1bdb45bac3b09e28e4f0cb09c97194 beauty3.pps
d807fb3cb1a0687e152d288171ab9b59 beauty6.pps
f017c65c7b5d14df11c5e0e4f0406562 CHINA_FEAR_US_3.pps
3cd8e3e80a106b0590a7b5eedddf4715 CHINA_FEAR_US_6.pps
a1940b31af27139a13dff852cb012a22 ChinainSyria.doc
e7ba5c209635607b2b0e38a00a822953 chinamilstrat1.doc
d273f090b96eca7c93387a03d9527d9b chinamilstrat2.doc
17d5acf49a4d65a4aacc362576dbaa12 chinamilstrength.pps
3c68ca564595e108920a0f105728fded China_Response_NKorea_Nuclear_Test1.pps
8c21aee21b6bfa12ecf6070a4532655a China_Response_NKorea_Nuclear_Test2.pps
533ce967d09189d27f38fe6ed4711099 chinascyberarmy2015_1.pps
9c9e5d09699821c53d68e957044ec6e8 chinascyberarmy2015_2.pps
c4f5d6ed36c3d51cb1b31f20922ce880 ChinasMilitaryIntelligenceSystemisChanging_1.doc
1fb7eece41b964517d5224b57073c5d4 ChinasMilitaryIntelligenceSystemisChanging_2.doc
1e620679c90563d46aa349e991d2e0f2
CHINA’S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_1.doc
a0177d2fd49d835244028e98449c77a5
CHINA’S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_1.pps
1e620679c90563d46aa349e991d2e0f2
CHINA’S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_2.doc
70c5267c56ded521c6f674a6a6649f05 CHINA’S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_2.pps
a1940b31af27139a13dff852cb012a22 ChinatoReceive_S-400_Missiles.doc
77ff734bc92e853b92595ddf999ee1ec China_two_child_policy_will_underwhelm1.doc
8c875542def907312fd92d10746c230c China_two_child_policy_will_underwhelm1.pps
e98b1ed80ba3a3b6b0809f04536e9753 ChinaUS_1.pps
36581da1d10ba6382a63e7046c21dd8d ChinaUS_2.pps
9a7e499d7abfcbe7fb2a78cf1d7a2f10 chinesemilstrat_1.pps
40ace1c9394c95d7e9e1e80f24bd1a73 chinesemilstrat_2.pps
71d59036f84aba8e60aa8785e3883372 cppcc_1.pps
04aff7c333055188219e290e58313d78 cppcc_2.pps
dffe28c9c4dc9e2e865e3237f4bc38c4 Dev_Kumar_Sunuwar.doc
ae27773e49fea122e3f8ce7a27e6c555 election.pps
86edf4fab125d8ccba85138f43b24def enggmarvels_1.pps
a8022594e81c74b22abca772eb89657c enggmarvels_2.pps
bc08d1bddf72369adceffbfc36f848df fengnew33.pps

2c70e1f152e2cb42bb29aadb66ece2ec fengnew36.pps
3a2be243b0c78e8689b34e2415d5e479 fengnew63.pps
2158cb891a8ecbaaa70a641a6529b787 fengnew66.pps
a1940b31af27139a13dff852cb012a22 final.doc
a1940b31af27139a13dff852cb012a22 FinancialCrisisChina.doc
884f76542f3972f473376c943daeaf8f futuredrones_1.pps
098c74c23ed73ac7bf7581fec2eb088d futuredrones_2.pps
915e5eefd145c59677a2a9eded97d114 gaokaonewreforms_1.doc
57377233f2a946d150115ad23bbaf5e6 gaokaonewschedule_1.pps
1c5b468489cf927c1d969484ddbdd8ea gaokaonewschedule_2.pps
fa2f8ec0ab22f0461e860394c6b06a68 harbin_1.pps
9a0534772ac23ff64e3c85b18fbec596 Heart_Valve_Replacement.doc
4ea4142bab2b90e5779df19616f7d8ca Implication_China_mil_reforms_1.doc
8a350d3f6fb359377d8939e1a2e033f3 Implication_China_mil_reforms_1.pps
f5e121671384fbd43534b8515c9e6940 ISIS_Bet_Part1.doc
3a83e09f1b751dc08f4b719ed51c3fbc ISIS_Bet_Part2.doc
8a1a10dcc6e2ac6b40a86d6ed20cf1bd japan_pivot_1.pps
72c05100da6b6bcbf3f96fee5cf67c3f japan_pivot_2.pps
ebe8efbad7f01b76465afaf474589c2f jtopcentrecomn.pps
165ae88945852a37fca8ec5224e35188 korea1.pps
38e71afcdd6236ac3ad24bda393a81c6 militarizationofsouthchinasea_1.pps
61f812a1924e6d5b4307313e20cd09d1 militarizationofsouthchinasea_2.pps
4595dbaeec06e3f9b466d618b4da767e MilitaryReforms1.pps
1de10c5bc704d3eaf4f0cfa5ddd63f2d MilitaryReforms2.pps
ce1426ffe9ad4439795d269ddcf57c87 MilReform_1.doc
1e620679c90563d46aa349e991d2e0f2 MilReform_2.doc
8d2f4e691f2e318f7162a3a5d397b29c MilReforms_1.pps
631d44688303be28a1b825aa1c9f3202 MilReforms_2.pps
fe78c037844ad08a9a79c85f46e68a67 my_lovely_pics_3.pps
d5a976cc714651711c8f067dd5e00709 my_lovely_pics_6.pps
657e9333a052f593b7c51c58917a1b1f my_photos_3.pps
e08bbed0aa4b21ae921d4dc5350789c7 my_photos_6.pps
141a8b306af8087df4feee15f571eb59 nail_art_3.pps
122d7dff33174e532063a16ae526208d nail_art_6.pps
d049a6f9e527a72a4b917eec1acbd6f9 netflix1.doc
09a478efd8c5aeef3a5395e3988f5059 netflix1.pps
d791f8d9495d5d5df0cedb8b27fb3b49 netflix2.doc
e7b4511cba3bba6983c43c9f9014a49d netflix2.pps
d01be8c3c027f9d6f0d93542dfe7ca97 nianshijiexiaoxuanshou2015.doc
040712ba00b32cc19e1938e14e732f59 North_Korea_Nuclear_Test_1.doc
3b0ca7dafb94333234e4f1330a1699da North_Korea_Nuclear_Test_2.doc
1e620679c90563d46aa349e991d2e0f2 Obama_Gift_China_1.doc
6f327b93279f3ce39f4fbe7a610c3cd2 Obama_Gift_China_1.pps
1e620679c90563d46aa349e991d2e0f2 Obama_Gift_China_2.doc
58179b5cf455e2bcac396c697cd43050 Obama_Gift_China_2.pps
fa94f2843639f7afec3c06799a8d222e PAK_CHINA_NAVAL_EXERCISEn.doc
4d2bde1b3985d1e1088801d92d1d6ca9 pension_1.pps
9a0534772ac23ff64e3c85b18fbec596 Reconciliation_China's_PLAN.doc
2c9b4d460e846d5814c2691ae4591c4f Stewardess1.doc
dab037a9e02978bcd275ddaa15dab01d stewardess1.pps

007c9c29786d0af81caf437fe626c6fe Stewardess2.doc
8aae16b5e64445703d939bc7923ae7b7 stewardess2.pps
036a45983df8f81bf1875097fc026b04 syria_china.pps
a8b9a32723452d27257924a737ec1bed TaiwanDiplomaticAccess_1.pps
f16ee3123d5eb21c053ac95e7cd4f203 TaiwanDiplomaticAccess_2.pps
71ce64fee9cd323828a44e9228d2736b tibetculture_1.pps
b5e5e428b31a8affe48fdf6b8a253dc6 tibetculture_2.pps
d64efa0b8c091b8dbed3635c2b711431 underestimatingUS_1.pps
543fe62829b7b9435a247487cd2a9672 underestimatingUS_2.pps
807796263fd236a041f3633ac578140e UruguayJan-Jun_1o.pps
98e7dc26531469e6b968cb422371601a uruguayjan-jun_1.pps
7eb1b6fefe7c5f86dcc914056928a17b UruguayJan-Jun_2o.pps
7660c6189c928919b0776713d2755db2 uruguayjan-jun_2.pps
7c4c866cf78be30229b75a3301345f44 UruguayJul-Dec_1o.pps
a4fcf3a441865ae17f2c80ff7c28543d uruguayjul-dec_1.pps
dba585f7d5fc51566c663bd738de2c33 UruguayJul-Dec_2o.pps
f7905a7bd6483a12ab36071363b012c3 uruguayjul-dec_2.pps
409e3368af2add71265d2811aa9d6817 US_China.doc
5a89f11f4bb3b5637c731e206f807ff7 us_srilanka_relations_1.pps
7f50d3f4eabffe7225a2d5f0c91009c8 us_srilanka_relations_2.pps
3d01d2a42450064c55574d853c086f9a WILL_ISIS_INFECT_BANGLADESH.doc
1538a412fd4035954237c0b4c135fcba WILL_ISIS_INFECT_BANGLADESH.pps
eb0b18ecaa6f40e48970b08f3a3e6803 zodiac_1.pps
da29f5eeb39332a850f04be2906315c1 zodiac_2.pps

Domains and IPs

http://www.epg-cn[.]com
http://chinastrat[.]com
http://www.chinastrats[.]com
http://www.newsnstat[.]com
http://cnmilit[.]com
http://163-cn[.]org
alfred.ignorelist[.]com
http://5.254.98[.]68
http://43.249.37[.]173
http://85.25.79[.]230
http://10.30.4[.]112
http://5.254.98[.]68
http://microsofl.mooo[.]com
ussainbolt.mooo[.]com
ussainbolt1.mooo[.]com
updatesys.zapto[.]org
updatesoft.zapto[.]org

http://feeds.rapidfeeds[.]com/61594/
http://wgeastchina.steelhome[.]cn/xml.xml
http://hostmyrss[.]com/feed/players
http://feeds.rapidfeeds[.]com/81908/
http://feeds.rapidfeeds[.]com/79167/
http://feeds.rapidfeeds[.]com/61594/

Update: our friends from Cymmetria have released their analysis of the Dropping Elephant / Patchwork APT – make sure to check it as well for more data about the attacks.