|  |  |
| --- | --- |
| Input article | Dropping Elephant 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 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. |
| Reference  summary | The PDF describes research and analysis conducted by Kaspersky Lab on a threat actor group named Dropping Elephant, also known as Chinastrats and Patchwork. The key points are: - Dropping Elephant targets high-profile diplomatic and economic organizations related to China's foreign relations. They use spearphishing and watering hole attacks. - Two main infection vectors are used. One sends a document that phones home when opened, followed by an exploit document to install malware. The other uses a website that requires downloading a document to see full articles, which contains an exploit. - The malware is an AutoIT backdoor that downloads additional components. It steals documents and data like Chrome credentials. - Infrastructure analysis revealed the campaign has been ongoing since at least November 2015. Most victims were in Asia with a focus on Chinese interests. - The group reuses some publicly available tools but combines them effectively with social engineering for successful attacks against high-value targets. - The malware artifacts are not technically advanced, using basic exploits, powershell scripts, and open source tools. Keeping software patched prevents much of the malware. - Attribution analysis tied the group to a threat actor using the alias "Aleksandr Sirofimov" which has been linked to previous cybercrime campaigns since 2015. The group may originate from Eastern Europe. In summary, Dropping Elephant is a relatively new but active threat group that has been successfully targeting organizations related to China's foreign relations through simple but cleverly social engineered attacks. |
| Annotated  terminologies | Analysis; Kaspersky Lab; Dropping Elephant; China; Patchwork; targets; foreign relations; spear; hole attacks; two main infection vectors; Exploit; a website; additional components; documents; data; the campaign; LEAs; most victims; Chinese interests; the group. |

|  |  |
| --- | --- |
| prompting | Summarize the article into a coherent and complete abstract |
| Generated  summary  (ChatGPT) | The article discusses the activities of the Dropping Elephant cyber-espionage group, also known as "Chinastrats" and "Patchwork" targeting high-profile diplomatic and economic entities involved with China's foreign relations. The group primarily utilizes spear-phishing and watering hole attacks, leveraging social engineering tactics for infiltration. The infection vectors involve sending documents with embedded executables exploiting vulnerabilities such as CVE 2012 0158 and CVE 2014 6352. Once executed, the payload downloads additional components, facilitating data theft. The group employs various tools and techniques, including UPX-packed backdoors, PowerShell scripts, and resilient communications methods to evade detection. C2 analysis reveals the group's use of VPNs and IPs from ordinary ISPs, complicating attribution. The article underscores the efficacy of low investment, readily available offensive toolsets, combined with high-quality social engineering, in cyber-espionage operations. |
| ROUGE | rouge1: 39.89; rouge2: 17.11; rougeL: 26.06 |

|  |  |
| --- | --- |
| prompting | Summarize the article into a coherent and complete abstract that incorporates the provided keywords. |
| Generated  terminologies | the document; Dropping Elephant; Chinastrats; Patchwork; the attacks; spear |
| Generated  summary  (ChatGPT) | The Dropping Elephant, also known as Chinastrats and Patchwork, is a new threat actor targeting high profile diplomatic and economic targets involved in China's foreign relations. The actor uses spear phishing and watering hole attacks to infect victims with malware, stealing documents and data. The malware is usually UPX packed and downloads additional components from the attackers' servers. The backdoor also communicates with the C2 server, uploading stolen files. The attackers maintain social media accounts to reach wider targets and hide encrypted C2 server locations in legitimate websites. The article provides in-depth analysis of the attack methods and tools used by Dropping Elephant. |
| ROUGE | rouge1: 43.93; rouge2: 19.18; rougeL: 27.16 |

|  |  |
| --- | --- |
| prompting | Summarize the article into a coherent and complete abstract that incorporates the provided keywords. |
| Generated  terminologies | dropping elephant; Chinastrats; Patchwork; the group; spear phishing; people; foreign relations; a custom set; attack tools; the attacks; the first approach; APT; Microsoft Word; PowerPoint; the second approach; watering hole attacks; links; social engineering; website; Google+; Facebook; Twitter; the backdoor; commands; C2; the malware; iterations; directories; documents; extensions; C2 execution; additional malware; malware samples; the C2 server; C2 analysis; a backdoor; files; strings; a single obfuscation algorithm; a high level social engineering; a unique response; the espionage; time. |
| Generated  summary  (ChatGPT) | The article discusses a new threat actor known as Dropping Elephant, also referred to as Chinastrats and Patchwork, that is targeting high profile diplomatic and economic targets involved in China's foreign relations. The group uses spear phishing and watering hole attacks as their main infection vectors, with a focus on social engineering. The first approach involves sending spear phishing emails with documents containing embedded executables, while the second approach involves creating a website that downloads genuine news articles but also asks visitors to download a malicious artifact. The group also uses other approaches such as emailing links to their watering hole websites and maintaining social media accounts to reach wider targets. The article also discusses the attack tools used by Dropping Elephant, including a backdoor that downloads additional malware in the form of encoded PowerShell scripts. The group also hides control server locations in comments on legitimate websites. The article concludes by mentioning the group's resilient communications and the difficulty in obtaining a full overview of their campaign. Overall, the activities of Dropping Elephant demonstrate the effectiveness of low investment and ready made offensive toolsets combined with high quality social engineering. |
| ROUGE | rouge1: 50.69; rouge2: 19.44; rougeL: 27.65 |

红：标注术语

蓝：目标摘要

绿：不在上述、但有效

PDF 描述了卡巴斯基实验室对名为 Dropping Elephant（又名 Chinastrats 和 Patchwork）的威胁行为者组织进行的研究和分析。关键点如下：- Dropping Elephant 针对与中国外交关系有关的知名外交和经济组织。他们使用鱼叉式网络钓鱼和水坑攻击。- 使用两种主要感染媒介。一种发送一个打开后会回电的文档，然后发送一个漏洞文档来安装恶意软件。另一种使用需要下载文档才能查看完整文章的网站，其中包含漏洞。- 该恶意软件是一个 AutoIT 后门，可下载其他组件。它会窃取文档和数据，例如 Chrome 凭据。- 基础设施分析显示，该活动至少从 2015 年 11 月开始。大多数受害者都在亚洲，重点关注中国利益。- 该组织重用了一些公开可用的工具，但将它们与社会工程学有效结合，以成功攻击高价值目标。- 恶意软件工件在技术上并不先进，使用基本的漏洞、powershell 脚本和开源工具。保持软件修补可以防止大部分恶意软件。 - 归因分析将该组织与使用别名“Aleksandr Sirofimov”的威胁行为者联系起来，该别名自 2015 年以来一直与以前的网络犯罪活动有关。该组织可能来自东欧。总之，Dropping Elephant 是一个相对较新但活跃的威胁组织，它通过简单但巧妙的社会工程攻击成功地瞄准了与中国外交关系有关的组织。“，

A：

ROUGE scores: {'rouge1': 0.39893617021276595, 'rouge2': 0.1711229946524064, 'rougeL': 0.26063829787234044, 'rougeLsum': 0.2606382978718802}

BERT scores: {'precision': 0.86028, 'recall': 0.87897, 'f1': 0.86953}

"gpt3\_gen\_texts": ["The article discusses the activities of the Dropping Elephant cyber-espionage group, also known as "Chinastrats" and "Patchwork" targeting high-profile diplomatic and economic entities involved with China's foreign relations. The group primarily utilizes spear-phishing and watering hole attacks, leveraging social engineering tactics for infiltration. The infection vectors involve sending documents with embedded executables exploiting vulnerabilities such as CVE 2012 0158 and CVE 2014 6352. Once executed, the payload downloads additional components, facilitating data theft. The group employs various tools and techniques, including UPX-packed backdoors, PowerShell scripts, and resilient communications methods to evade detection. C2 analysis reveals the group's use of VPNs and IPs from ordinary ISPs, complicating attribution. The article underscores the efficacy of low investment, readily available offensive toolsets, combined with high-quality social engineering, in cyber-espionage operations."]

PDF 描述了卡巴斯基实验室对名为 Dropping Elephant（又名 Chinastrats 和 Patchwork）的威胁行为者组织进行的研究和分析。关键点如下：- Dropping Elephant 针对与中国外交关系有关的知名外交和经济组织。他们使用鱼叉式网络钓鱼和水坑攻击。- 使用两种主要感染媒介。一种发送一个打开后会回电的文档，然后发送一个漏洞文档来安装恶意软件。另一种使用需要下载文档才能查看完整文章的网站，其中包含漏洞。- 该恶意软件是一个 AutoIT 后门，可下载其他组件。它会窃取文档和数据，例如 Chrome 凭据。- 基础设施分析显示，该活动至少从 2015 年 11 月开始。大多数受害者都在亚洲，重点关注中国利益。- 该组织重用了一些公开可用的工具，但将它们与社会工程学有效结合，以成功攻击高价值目标。- 恶意软件工件在技术上并不先进，使用基本的漏洞、powershell 脚本和开源工具。保持软件修补可以防止大部分恶意软件。 - 归因分析将该组织与使用别名“Aleksandr Sirofimov”的威胁行为者联系起来，该别名自 2015 年以来一直与以前的网络犯罪活动有关。该组织可能来自东欧。总之，Dropping Elephant 是一个相对较新但活跃的威胁组织，它通过简单但巧妙的社会工程攻击成功地瞄准了与中国外交关系有关的组织。“，

本文讨论了 Dropping Elephant 网络间谍组织（又名“Chinastrats”和“Patchwork”）的活动，该组织针对与中国外交关系有关的知名外交和经济实体。该组织主要利用鱼叉式网络钓鱼和水坑攻击，利用社会工程学策略进行渗透。感染媒介包括发送嵌入可执行文件的文档，这些可执行文件利用了 CVE 2012 0158 和 CVE 2014 6352 等漏洞。一旦执行，有效载荷就会下载其他组件，从而帮助窃取数据。该组织使用各种工具和技术来逃避检测，包括 UPX 打包的后门、PowerShell 脚本和弹性通信方法。C2 分析显示该组织使用普通 ISP 的 VPN 和 IP，使归因变得复杂。本文强调了低投资、随时可用的攻击工具集与高质量社会工程学相结合在网络间谍行动中的有效性

本文讨论了一个名为 Dropping Elephant 的新威胁行为者，也称为 Chinastrats 和 Patchwork，其目标是涉及中国外交关系的知名外交和经济目标。该组织使用鱼叉式网络钓鱼和水坑攻击作为其主要感染媒介，重点是社会工程学。第一种方法是发送带有嵌入可执行文件的文档的鱼叉式网络钓鱼电子邮件，**而第二种方法是创建一个下载真实新闻文章的网站，但也要求访问者下载恶意工件。**该组织还使用其他方法，例如通过电子邮件发送指向其水坑网站的链接并维护社交媒体帐户以覆盖更广泛的目标。本文还讨论了 Dropping Elephant 使用的攻击工具，包括一个以编码的 PowerShell 脚本形式下载其他恶意软件的后门。该组织还在合法网站的评论中隐藏控制服务器位置。文章最后提到了该组织的弹性通信以及获得其活动全面概述的难度。总体而言，Dropping Elephant 的活动证明了低投资和现成的攻击工具集与高质量社会工程学相结合的有效性。

A+SFT

ROUGE scores: {'rouge1': 0.43930635838150295, 'rouge2': 0.1918604651162791, 'rougeL': 0.2716763005780347, 'rougeLsum': 0.27167630057761194}

BERT scores: {'precision': 0.85545, 'recall': 0.89718, 'f1': 0.87582}

"prediction": "the document; Dropping Elephant; Chinastrats; Patchwork; the attacks; spear",

"gpt3\_gen\_texts": ["The Dropping Elephant, also known as Chinastrats and Patchwork, is a new threat actor targeting high profile diplomatic and economic targets involved in China's foreign relations. The actor uses spear phishing and watering hole attacks to infect victims with malware, stealing documents and data. The malware is usually UPX packed and downloads additional components from the attackers' servers. The backdoor also communicates with the C2 server, uploading stolen files. The attackers maintain social media accounts to reach wider targets and hide encrypted C2 server locations in legitimate websites. The article provides in-depth analysis of the attack methods and tools used by Dropping Elephant."]

A+SFT+RL

"gpt3/lexical/rouge\_rouge1": 0.5069124423963134, "gpt3/lexical/rouge\_rouge2": 0.19444444444444442, "gpt3/lexical/rouge\_rougeL": 0.2764976958525346, "gpt3/lexical/rouge\_rougeLsum": 0.2764976958525346,

"generated\_text": "dropping elephant; Chinastrats; Patchwork; the group; spear phishing; people; foreign relations; a custom set; attack tools; the attacks; the first approach; APT; Microsoft Word; PowerPoint; the second approach; watering hole attacks; links; social engineering; websites; Google+; Facebook; Twitter; the backdoor; commands; C2; the malware; iterations; directories; documents; extensions; C2 execution; additional malware; malware samples; the C2 server; C2 analysis; a backdoor; files; strings; a single obfuscation algorithm; a high level social engineering; a unique response; the espionage; time.",

"gpt3\_generated\_text": ["The article discusses a new threat actor known as Dropping Elephant, also referred to as Chinastrats and Patchwork, that is targeting high profile diplomatic and economic targets involved in China's foreign relations. The group uses spear phishing and watering hole attacks as their main infection vectors, with a focus on social engineering. The first approach involves sending spear phishing emails with documents containing embedded executables, while the second approach involves creating a website that downloads genuine news articles but also asks visitors to download a malicious artifact. The group also uses other approaches such as emailing links to their watering hole websites and maintaining social media accounts to reach wider targets. The article also discusses the attack tools used by Dropping Elephant, including a backdoor that downloads additional malware in the form of encoded PowerShell scripts. The group also hides control server locations in comments on legitimate websites. The article concludes by mentioning the group's resilient communications and the difficulty in obtaining a full overview of their campaign. Overall, the activities of Dropping Elephant demonstrate the effectiveness of low investment and ready made offensive toolsets combined with high quality social engineering."]

**~~目标摘要：~~**~~PDF 描述了卡巴斯基实验室对名为 Dropping Elephant（又名 Chinastrats 和 Patchwork）的威胁行为者组织进行的研究和分析。关键点如下：- Dropping Elephant 针对与中国外交关系有关的知名外交和经济组织。他们使用鱼叉式网络钓鱼和水坑攻击。- 使用两种主要感染媒介。~~一种发送一份打开后会回电的**文档**，然后发送一个**漏洞**文档来安装恶意**软件**。另一种使用需要下载文档才能查看完整文章的网站，其中包含漏洞。- 该恶意软件是一种 AutoIT 后门，可下载其他组件。它会窃取文档和数据，例如 Chrome 凭据。- 基础设施分析显示，该活动至少从 2015 年 11 月开始。大多数受害者都在亚洲，重点关注中国利益。- 该组织重用了一些公开可用的工具，但将它们与社会工程学有效结合，以成功攻击高价值目标。- 恶意软件工件在技术上并不先进，使用基本的漏洞、powershell 脚本和开源工具。保持软件修补可以防止大部分恶意软件。 - 归因分析显示，该组织与使用别名“Aleksandr Sirofimov”的威胁行为者有关，该别名自 2015 年以来一直与以前的网络犯罪活动有关。该组织可能来自东欧。总之，Dropping Elephant 是一个相对较新但活跃的威胁组织，它通过简单但巧妙的社会工程攻击成功地瞄准了与中国外交关系有关的组织。

**~~A：~~**~~本文讨论了 Dropping Elephant 网络间谍组织（又名“Chinastrats”和“Patchwork”）的活动，该组织针对与中国外交关系有关的知名外交和经济实体。该组织主要利用鱼叉式网络钓鱼和水坑攻击，利用社会工程学策略进行渗透。~~感染媒介包括发送嵌入可执行文件的文档，这些可执行文件利用了 CVE 2012 0158 和 CVE 2014 6352 等漏洞。一旦执行，有效载荷就会下载其他组件，从而帮助窃取数据。该组织使用各种工具和技术来逃避检测，包括 UPX 打包的后门、PowerShell 脚本和弹性通信方法。C2 分析显示该组织使用 VPN 和普通 ISP 的 IP，使归因变得复杂。本文强调了低投资、随时可用的攻击工具集与高质量社会工程学相结合在网络间谍行动中的有效性。

**~~A+SFT：~~**~~Dropping Elephant 又名 Chinastrats 和 Patchwork，是一个新型威胁行为者，主要针对涉及中国外交关系的知名外交和经济目标。该行为者使用鱼叉式网络钓鱼和水坑攻击，用恶意软件感染受害者，窃取文件和数据。~~该恶意软件通常经过 UPX 打包，并从攻击者的服务器下载其他组件。后门还与 C2 服务器通信，上传被盗文件。攻击者维护社交媒体帐户以接触更广泛的目标，并将加密的 C2 服务器位置隐藏在合法网站中。本文对 Dropping Elephant 使用的攻击方法和工具进行了深入分析。

**~~A+SFT+RL：~~**~~本文讨论了一个名为 Dropping Elephant 的新威胁行为者，也称为 Chinastrats 和 Patchwork，其目标是涉及中国外交关系的知名外交和经济目标。该组织使用鱼叉式网络钓鱼和水坑攻击作为其主要感染媒介，重点是社会工程学。~~第一种方法是发送带有嵌入可执行文件的文档的鱼叉式网络钓鱼电子邮件，而第二种方法是创建一个下载真实新闻文章的网站，但也要求访问者下载恶意工件。该组织还使用其他方法，例如通过电子邮件发送指向其水坑网站的链接并维护社交媒体帐户以覆盖更广泛的目标。本文还讨论了 Dropping Elephant 使用的攻击工具，包括一个以编码的 PowerShell 脚本形式下载其他恶意软件的后门。该组织还在合法网站的评论中隐藏控制服务器位置。文章最后提到了该组织的弹性通信以及获得其活动全面概述的难度。总体而言，Dropping Elephant 的活动证明了低投资和现成的攻击工具集与高质量社会工程学相结合的有效性。

"article": " Dropping Elephant 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 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 Tools1. 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\u2019s 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 power shell command line \u201cscripts\u201d. 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 Comment Crew, 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.url Pro\ufb01le and Geography3/102016/7/14Victim Pro\ufb01le and GeographyThe Dropping Elephant actor - SecurelistWe 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\u2019s Republic of China) could be for a variety of reasons \u2013 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.ConclusionCampaigns 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\u00b4s patch for exploit CVE 2014 1761 just warns the user not to allow the execution of the suspicious file.url Dropping Elephant actor - SecurelistDropping 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.GenericAs 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.comMore information on how Kaspersky Lab technologies protect against such cyberespionage attacks is available on Kaspersky 13\_Five\_Year\_Plan\_2016 20 1.pps Reconciliation\_China\u2019s\_PLAN.doc url url url url url cn[.]org alfred.ignorelist[.]com url url url url url url ussainbolt.mooo[.]com ussainbolt1.mooo[.]com updatesys.zapto[.]org updatesoft.zapto[.]orgC2 redirectors (with obfuscated comments)url url url url url url Dropping Elephant actor - SecurelistUpdate: our friends from Cymmetria have released their analysis of the Dropping Elephant / Patchwork APT \u2013 make sure to check it as well for more data about the attacks.Related PostsOPERATION DAYBREAKCVE-2016-4171 \u2013 ADOBE FLASH ZERO-DAY USED THREATSurl ",