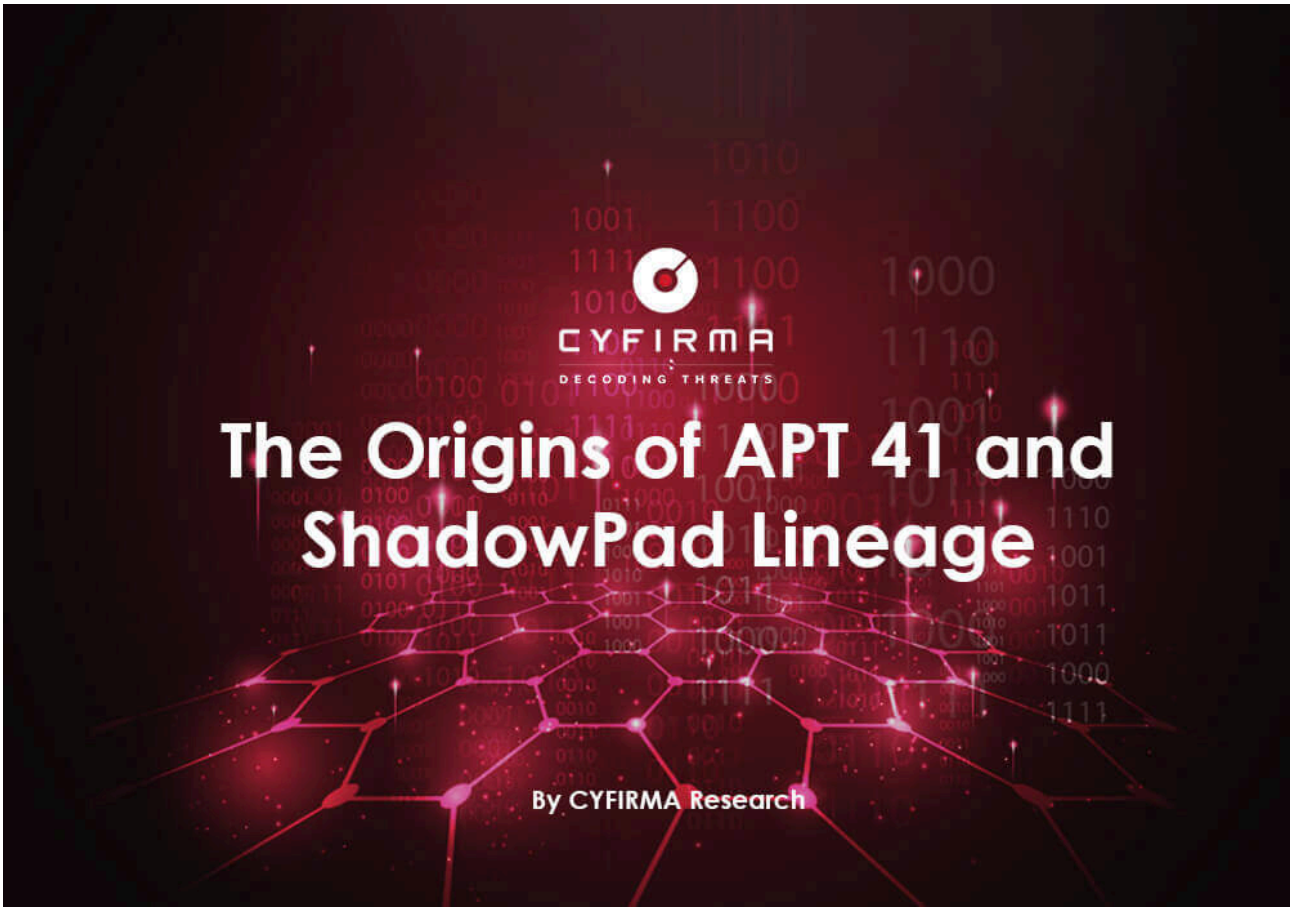
The Origins of APT 41 and ShadowPad Lineage - CYFIRMA

Archived: 2026-04-05 18:02:52 UTC

Published On : 2022-07-13



Introduction

When the CYFIRMA research team began its work on tracking APT41, it became apparent that there is a rich history to be learned first as part of any attempt to understand this APT. This history allowed us to trace the lineage of the ShadowPad modular malware kit back to the early 2000s while finding its likely exclusive use in the current day by the reformed Chinese military. This paper will focus mainly on tracking early history, connections, and legacies to provide useful CTI context to current-day TTPs and campaigns. While there have been many works published over more than a decade about individual pieces of this puzzle, to our knowledge, there is no publicly available work covering the entire story.

There are many more names involved (see figure below for a few), but we have chosen to follow only two main characters for this story. Tan Dailin, known as Meigui – Wicked Rose, also translated as Withered Rose, and known author of PlugX RAT – ‘whg’. The latter was not a permanent member of the NCPH group but played a major role in developing important tools leading up to the ShadowPad malware that is used today.

Between 2007 and 2008 this story is branching out in multiple directions such as Winnti or Chengdu 404 conspiracy, all of which are equally fascinating. For clarity, we focused only on ShadowPad-related branches.

Early Days

The story begins in 1994 when Tan Dailin aka Rose started a hacking group with his friends that would eventually form Network Crack Program Hacker Group (NCPH) which later grew into today's APT41. Not much is known about the very early hacking activity of Rose or the group members. However, according to Rose's archived blog, he grew up very poor and learned programming from books borrowed from the school library. He did not own a computer and learned by writing code with pencil and paper before being able to use computers at a local "third-rate" university. There he got into hacking and met like- minded friends and it is here that his talent was later discovered by the PLA (People's Liberation Army of China). According to Alan Paller's testimony before US Senate, Rose was contacted by Sichuan Military Command Communication Department to sign up for Chengdu Military Command Network Attack/Defense Competition. His team won this competition, received intensive 30-day training from the state, and went on a winning streak competing against other provinces netting 20,000RMB in prize money. This is also when they reportedly received an "undisclosed" sponsor paying the group 2,000 RMB a month to work on targeted attacks. After completing targeted attacks, they would receive 5,000 RMB bonuses. That was a lot of money back in 2006 China. Allan Paller's testimony also mentions Tan Dailin and his group starting a company to develop hacking tools for PLA. This company was likely CNASM, through which they offered many of the tools they developed. Such contracting gigs, according to available intelligence, are in line with the current state of the Chinese nation-state-sponsored cyber warfare program. Similar to other nations like USA or Israel, there are several private companies contracted to support state efforts with tools and manpower in cyberspace.

Zero-Days

In 2006, the group gained international media notoriety through a series of 0-day exploits and attacks against vulnerabilities in MS Office products, targeting Japan, the USA, and the UK. The broader series of cyber-attacks from China was named Titan Rain by the US government. These attacks carried a payload of GinWui backdoor/rootkit developed by Rose and whg. Although Titan Rain included multiple Chinese threat actors and campaigns, Tan Dailin's group stood above the rest with multiple 0-day exploits and precisely executed attacks. Notable modus operandi during these campaigns included carefully crafted spear-phishing emails targeted at single individuals and often sent out only one or two. This is a testament to a high success rate and implies stealth priority, offering another clue to espionage motivation and likely PLA contracts in place.

In 2007, Time magazine interviewed the NCPH group where they confessed to much of the above. They also ran a now-defunct blog www.ncph.net where they openly talked about their activities. Additionally Rose himself ran a personal blog at mghacker.com.


网络：破解：程序：黑客：Exploits：好软推荐：学习心情：BBS：留言本：
N C P H
业务介绍
※ 网站建设业务 ※
承接各类静、动态网站设计制作及网站更新维护。Rodag、asadmin、wrphp、ntel具有开发中小型网站的丰富经验，良好的网页设计师素质，曾为企业、机关单位、学校及个人设计制作网站、宣传页面达50余个，良好的团队合作能力。
※ 软件破解业务 ※
承接各类软件的破解业务，KuNgBiM、rack、ckdog、pksoft可谓国内知名的软件破解人员，为国内多个破解组织主要成员，能独立破解各种工程软件，外挂软件，黑客软件，对加密狗也有一定的研究，同时承接软件汉化业务！
※ 程序设计业务 ※
承接软件设计业务，W.Z.T、gramer、stolo、pocill低调的程序人，独立完成了多个程序设计，能熟练运用汇编、c/c++,vc++,vb,delphi,对数据库编程有一定的研究！能写一些木马软件，系统软件，工程软件，黑客工具，软件修改等。
※ 网络攻防业务 ※
承接网络攻防业务，Rose－－玫瑰、Ckfang、mghk、Flying Cat、ickey都有各自的特长，分别对windows、linux、unix系统有很深的研究，擅长各种脚本注入，能独立分析asp、php、jsp代码，挖掘脚本漏洞！能用perl写一些脚本程序，并且有一定的编写黑客软件，EXP，木马软件，漏洞利用工具的能力。精通已知漏洞，并独立开发研究出一些未公开漏洞。拥有我们独有的入侵方式，以及安全防护措施，能承接各种网络安全检测，系统安全服务，黑客程序开发等服务。
= N.C.P.H 原创软件内置广告条正在招商中，请与我们联系 =
NCPH © 2005-2006 // NCPH STUDIO WWW.NCPH.NET //
工作室业务QQ：
商业群：18305666 商业群II：21718940 技术群I：15796645
技术群III：21717474 技术群IV:8359236(新)
By [N.C.P.H]

APT41 Days

After 2007, all public online presence of the group and the TTPs they used started to disappear. Later, they also started removing old traces and tools even from their business CNASM website, which eventually disappeared too. All this while attacks from China increased in volume and sophistication. This makes sense and the initial willingness to stay in the spotlight of media attention was very likely quickly realized as a big mistake by the group and PLA alike.

Since then, activity initially traced to the NCPH group started to branch out and their TTPs overlapped with new ones, researchers began to track this cluster of activity under APT41. Major confusion was caused by this nexus of activities conducting covert espionage campaigns while simultaneously hacking for personal gain. According to the US Department of Justice 2020 report, members of APT41 went on a decade-long cybercrime spree. This included hacking video games for profit, namely generating in-game items with real- world monetary value or straight out hacking the gaming companies. Then there is Chengdu 404 racketeering conspiracy, where APT41 members used Chengdu 404 Network Technology company as a front to hack and blackmail over 100 companies, organizations, and individuals across the world, but mainly in East and Southeast Asia. Many of these gaming industry attacks were also linked to the Winnti group and the tool Winnti for Windows – a Remote Access Trojan (RAT).

This aligns with the hypothesis of a legitimate contracting company, led by Tan Dailin aka Rose and contracted by PLA to deliver hacking tools and conduct targeted attacks. At the same time, they were likely enjoying special privileges to conduct cyber-attacks for personal gain as long as their victims were outside China and avoiding its allies (Russia, DPKR, Iran, etc.) since those were curiously missing from the map of their victims. And it explains the unusual overlap of TTPs and tools like PlugX used in cutting-edge nation- state covert campaigns along with for-profit hacking, long before the trend of using commodity malware and TTPs that we see today.

ShadowPad and Chinese Military Reform

When tracking ShadowPad's history and activities, various elements of previously used tools like PlugX or Winnti for Windows, came together as part of one "masterpiece" modular malware kit. Using a unified, versatile framework is cost and resources effective for any organization, thereby prompting developers to focus on maintaining and developing its capabilities further, while users can enjoy the ease of use by conducting most of the attacks through a single tool. Assuming said users are military officers, this is invaluable in being able to train as many people as possible to conduct cyberspace operations.

Furthermore, unlike PlugX, which was and still is used widely by many groups, ShadowPad appears to be designed for specific and limited users only. Specifically, the People's Liberation Army Strategic Support Force (PLA SSF), founded in 2015 as part of Chinese military reform. Timelines seem to check out and ShadowPad has, through its encrypted plugin design and ID system, garnered robust control over how and by whom is it being used.

Furthermore, while studying the web archives about NCPH and early APT41 activities, their keen interest in Japanese popular culture and video games is very apparent. Also discernible is a long history of focus on Japanese targets since at least 2003, which later expands to other East and Southeast Asian targets, meanwhile still majorly targeting gaming companies. Considering this valuable long-term knowledge of the local cyber-landscape with all other circumstantial evidence, it is suggested that their initial PLA SSF contractors were units (known as Tick and Team Tonto) focusing on East Asia and Japan. This would explain ShadowPad being initially used almost exclusively on organizations in this region and by these APTs. Since then, ShadowPad was detected more widely across the world, suggesting growing adoption across PLA SSF.

GinWui/NCHP Remote Control

GinWui is a name given to the “NCPH remote control” tool by western researchers and it is the first known malware toolkit created by members of the NCPH group. It was extensively used during the 2006 0-day attacks on MS Office products and was co-developed by both Rose and whg during their NCPH days.

Note: For purpose of this article names “GinWui” and “NCPH tool” are used interchangeably as they both refer to the same software.

Notable is the extensive use of the early DLL loading technique, that the group developed for GinWui. This technique has been gradually developed and improved and is used in its latest iterations to this day by PlugX and even ShadowPad plugins.

The group offered GinWui demo version for free on their website together with other tools that they had developed. The full version was most likely available only to members and PLA which allegedly contracted its development, including version 3.0 of the tool that is formally branded as the “NCPH remote control” rootkit by the NCPH group.

Through the magic of internet archives, we were able to find all tools offered on the group’s official CNASM company website.


MALWARE

Figure 3.: "NCPH remote control" tool versions marked in the red box

While looking at the other and older tools available on the website, it is clear that many of them were the building blocks of NCPH remote control and ended up being absorbed into it. At the end of 2005, the group consolidated everything and continued developing it as one tool for some time.

Each version came with promotional screenshots and release notes.

Fig. x GinWui/NCPH3.0 screenshot

Release notes (translated):

- Support batch file breakpoint upload and download.
- Support remote process and registry management
- Support remote more hardware and software information o Support screenshot operation with SHELL command
- Support … It's better to see for yourself.

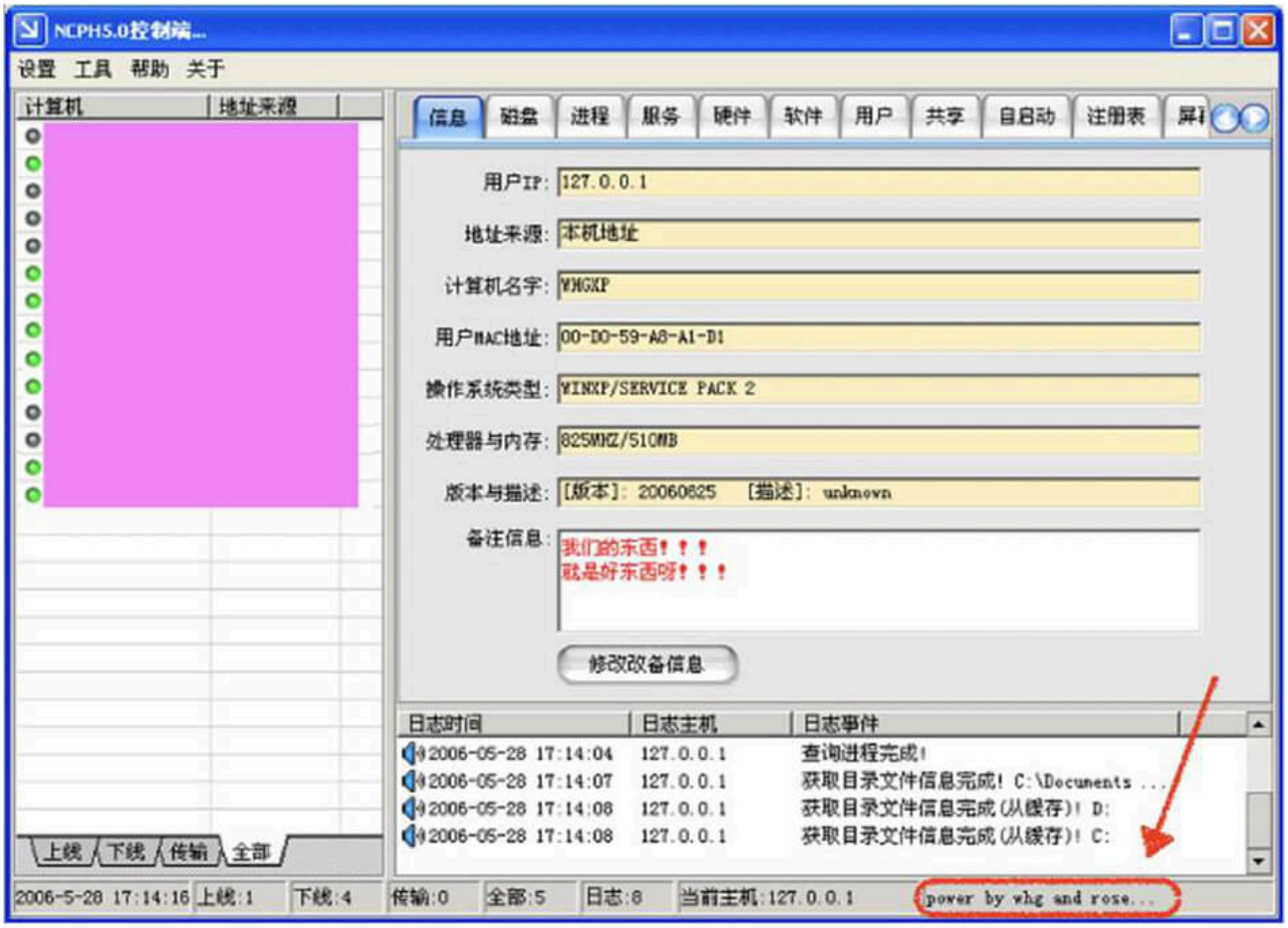


Fig. x GinWui/NCPH5.0 - *“power by whg and rose”*

Release notes (translated):

Modification record

- 2006-05-28 Release the latest version of 5.0
- 2006-05-30 Solve the problem of 5.0 mouse funnel.
- 2006-05-30 Solve the problem that 5.0 can’t be online, more than 10 characters domain name can not be online.

I. Technical features

- Controlled side using DLL design method
- No services on the controlled side (the controlled side does not rely on services to start, so do not add any services)
- Controlled side to hide files, registry, modules, port connection information
- The controlled side of self-protection with guarding capabilities
- The controlled side penetrates the personal firewall by injecting IE process.
- The controlled side of the bounce connection, support for domain names, IP.

II. Service content and console function settings

- File management functions of the major categories (batch upload, download, delete, support directory, breakpoint sequential transfer)
- Process management, you can browse, take module information, terminate the process.
- Service management, can browse, delete, stop, start specified services
- SHELL command, can execute any DOS command and return the result.
- Can lock, restart, shut down the controlled computer, can uninstall the server
- Logging, comprehensive operation records, as well as the ability to view the cause of failure
- Screenshot, camera, self-start, user, shared information, hardware and software information, etc.
- Support voice prompts.

Fig. x GinWui/NCPH6.0.1

Release notes (translated):

Origins of APT41 and ShadowPad lineage

Fig. x GinWui/NCPH6.0.1

ncph6.0 Features Introduction

- Disk management, upload and download, process execution, support for breakpoints, support for multi-language view and use. 2) process management, view process, end this process
- Service management, view services, start services, stop services
- Remote control, view screen, control screen

- cmdshell, command execution, imitate windows cmdshell
- System command, send message, shutdown and restart, uninstall.

This version is very stable and removes unnecessary hook hiding.

This software is only suitable for managing authorized remote computers, please do not use it for illegal activity, to prevent illegal use, do some functional restrictions. ncph will release the next version with improved ease of use and high stability, so stay tuned.

As previously noted, in 2007 all versions of the NCPH tool were removed from the website and only other older tools remained. CNASM company later continued to develop and offer other tools on their website until at least 2013.

SockMon – Powerful process and network monitoring utility.
VirTest – Promoted as a tool for developers to test their software for antivirus detection.
PM – Universal Port Mapper, remote control tool allowing for mapping internal network IPs and ports to internet-facing IPs and ports as described on their page.

> 实际应用，将内网"192.168.0.100:3389"映射到"221.10.254.92:3380"。
> 在"192.168.0.100"执行命令: PM -C 3389 221.10.254.92:12345
> 在"221.10.254.92"执行命令: PM -S 3380 12345
> 用远程桌面连接"221.10.254.92:3380"即可控制内网机器192.168.0.100:3389
> 12345端口是数据中转端口，可以随意设置。

Translated: *Practical application, the internal network "192.168.0.100:3389" mapped to "221.10.254.92:3380".*
Execute the command in "192.168.0.100": PM -C 3389 221.10.254.92:12345
Execute the command at "221.10.254.92": PM -S 3380 12345
Use remote desktop connection "221.10.254.92:3380" to control the intranet machine 192.168.0.100:3389 Port 12345 is the data transit port, you can set it as you like.

> 超级跳板，采用组合映射，使控制目标机在内网与外网中交替，达到隐藏控制者真实地址的目的。
> 最后映射为，内网（控制端）->公->内-公->内....->目标机，最后，最前端的内网用户成了控制者的替死鬼。

Translated: *The super springboard, using a combination of mapping, so that the control target machine alternates between the intranet and the extranet, to achieve the purpose of hiding the controller's real address.*
The final mapping is intranet (controller)->public->internal-public->internal …. -> target machine, and finally, the most front-end intranet user becomes the scapegoat of the controller.

It is very clear that this company was not developing the usual admin and dev utilities even after removing GinWui/NCPH Tool rootkits. And with high confidence, we can say that they were used in developing PlugX.

PlugX

Known and active since 2008, this malware was extensively analyzed by researchers over the years in multiple independent papers. It is still an active malware framework and as its name suggests, it is a modular backdoor

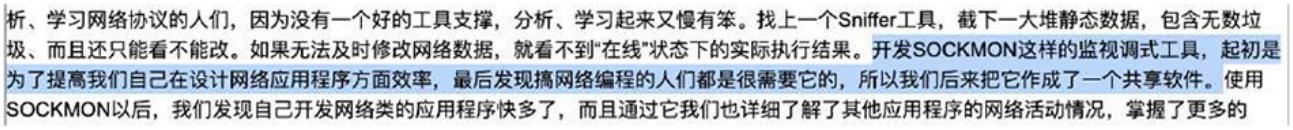
with a plethora of available plugins to modify it according to the attackers' needs. The same modular design gave PlugX over decade-long longevity.

There are a few direct links of PlugX to its predecessor GinWui and NCPH members. Number one is utilizing an improved DLL loading technique previously used in GinWui. The group has been observed changing this technique to avoid detection over the years. For example, in 2015 it was using a legitimate Samsung application for DLL side-loading.

Another conclusive link to whg was hidden directly in the early PlugX samples, specifically in file paths after debugging:
C:\Users\whg\Desktop* C:\Documents and Settings\whg*

If the username whg in the file path was not enough, the same was observed in other tools SockMon and WHGSniff available on the CNASM website. As noted, SockMon was actively developed and available at least until 2012 specifically by whg himself.

SockMon appears to absorb WHGSniff later on and according to the creators' own description of the old 2005 version, it was used to develop other "network applications".


析、学习网络协议的人们，因为没有一个好的工具支撑，分析、学习起来又慢有笨。找上一个Sniffer工具，截下一大堆静态数据，包含无数垃圾、而且还只能看不能改。如果无法及时修改网络数据，就看不到"在线"状态下的实际执行结果。开发SOCKMON这样的监视调式工具，起初是为了提高我们自己在设计网络应用程序方面效率，最后发现搞网络编程的人们都是很需要它的，所以我们后来把它作成了一个共享软件。使用SOCKMON以后，我们发现自己开发网络类的应用程序快多了，而且通过它我们也详细了解了其他应用程序的网络活动情况，掌握了更多的

Translated: *"We developed SOCKMON as a monitoring tool initially to improve our own efficiency in designing network applications, but eventually we found that people in network programming needed it, so we made it a shareware."*

Over the years two major pain points of the old design and distribution of PlugX became apparent. The design flaw was the inability to switch plugins during runtime, thereby severely limiting its agility and unnecessarily prolonging time spent getting a foothold in the victim network, risking detection.

Another problem was its wide distribution among Chinese threat actors, resulting in high detection rates and susceptibility to defensive measures, which severely hindered the malware's ability to carry out covert espionage campaigns. On the technical side of the distribution, authors/operators had limited to no control over the usage of this PlugX framework and its plugins. If anyone was able to get their hands on the binaries, they were able to start using them with all plugins without paying or restrictions. We believe those were the main reasons to develop a new version, which addressed these issues and that's exactly what ShadowPad did.

ShadowPad

Used at least since 2017, it is a direct descendant of PlugX, as conclusively proven by researchers. In a nutshell, early ShadowPad did not change much the TTPs used by PlugX and its plugins. It was instead addressing issues concerning agility, distribution, and usage control as faced by PlugX. They were both nearly identical modular malware toolkits when ShadowPad first appeared. Even today, ShadowPad samples are still using the time-proven, albeit improved, DLL loading technique. It is a common thread ever since the first known version of GinWui was discovered during the 2006 MS-Office 0-day attacks. What set it really apart was switching plugins during runtime capability, which had changed the attack patterns.

Eventually, few researchers were able to analyze mistakenly published early samples of ShadowPad and discovered ID strings. Each of these samples had different and limited configurations or capabilities – several plugins, based on specific IDs, etc. Furthermore, these plugins are packed in a proprietary format. Also, they are encrypted with a custom algorithm and decrypted in memory, meaning if it gets into unauthorized hands, it will be severely limited.

This feature allows very tight control of ShadowPad which provides for substantially better monetization. At the same time, it is very much in line with what the military would desire in the modern hacking toolkit.

Conclusion And Summary

Various research papers offer slightly different stories about ShadowPad and APT41. Even CYFIRMA's own research cannot offer conclusive attribution due to countless TTP overlaps between multiple threat actors that are more or less loosely affiliated with Dan Tailin. Some hacking for personal gain, some stealing secrets for the state, and some indulging in both, thereby effectively muddying the waters to the point where we will likely never know the definitive and complete story. Following the facts from US government investigation reports and proven links, we can paint a somewhat clear picture of who the threat actors are, what are their motivations, and where they came from.

N.C.P.H. was a group of hackers led by Tan Dailin who met at University and were entirely motivated by passion and bragging rights among peers. Later, after being scouted by the local military branch at a young age, they received state-sponsored training and were nurtured into highly skilled professionals that we know today as APT41.

CNASM – a private company developing hacking tools for PLA that started in the early 2000s – was founded by Tan Dailin and where whg is known to have crafted multiple malicious programs. The perpetrators here were still largely motivated by passion and bragging rights, including publicly boasting about their exploits. That eventually changed around 2007, when after conducting campaigns for PLA, the group's old public posts started to disappear.

APT41 today is most likely a private company, possibly rebranded CNASM, or multiple companies created by employees of former CNASM. Contracted by PLA and later PLA SSF to develop cyber tools for military purposes. And, at least in the early days, also contracted to conduct campaigns on behalf of the military. At the same time company employees and affiliates were allowed to conduct attacks for personal gain as long as it was not targeting China and its allies. Herein was a clear switch from passion to money-motivated cybercrime along with covert operations for the state.

GinWui/NCPH tool is the first known toolkit developed by CNASM. Notable for introducing signature DLL loading technique and using 0-day MS Office exploits during 2006 attacks on Japanese and US targets.

PlugX is a widely adopted and versatile modular malware toolkit used for state-sponsored espionage as well as in private hacking by various Chinese threat actors. The malware was notable for its plugin design and has been proven to be developed by whg.

ShadowPad is the latest modular malware toolkit developed by APT41 most likely directly for PLA SSF after the 2015 PLA reforms. It addresses many flaws noticed in PlugX and consequently, since its first appearance, it appears to be more widely adopted by state-sponsored actors.
