THREAT RESEARCH

Bitdefender

Security

Dissecting a Chinese APT Targeting Southeast Asian Government Institutions

www.bitdefender.com

EXECUTIVE SUMMARY

Bitdefender researchers are continuously monitoring APT groups and their activities around the world in an effort to gain better insights into their tactics, techniques and targeted victims. While some APT groups operate for financial profit, others have been attributed to nation states and may follow a political agenda. Forensic artifacts left behind by APT groups when using custom-built tools or specific payloads can sometimes point to a known actor but may also reveal additional information about how the groups operate after compromising a target.

When monitoring for activity of APT groups in the Asian region, Bitdefender researchers found signs of a complex and targeted espionage attack on potential government sector victims in South East Asia, carried out by a sophisticated Chinese APT group, judging from some of the forensic artifacts left behind. The operation was conducted over at least a few years, as the earliest signs of potential compromise date back to late 2018. While current forensic evidence follows the attack timeline up to 2020, a large number of C&C servers are inactive. It's likely the overall attacker-controlled infrastructure used in the attack is currently inactive, even though very few C&Cs have been found to still be operational.

This research focuses on dissecting an APT attack and providing a full report on the tools, techniques and procedures used by the sophisticated group during the attack. Bitdefender's investigation focuses on offering a detailed timeline of the attack by piecing all the forensic evidence together and creating a case study example. The report also provides a technical analysis of the tools used in this targeted attack and how the components were tied to each other.

The attack has a complex and complete arsenal of droppers, backdoors and other tools involving Chinoxy backdoor, PCShare RAT and FunnyDream backdoor binaries, with forensic artefacts pointing towards a sophisticated Chinese actor. Some of these open source Remote Access Trojans (RATs) are known to be of Chinese origin, along with some other resources set to Chinese. The FunnyDream backdoor is far more complex than the others, implementing a wide range of persistence mechanism and a large number of droppers, suggesting it's custom-made.

The earliest signs of attack date back to November 2018, followed by an increase in activity by the Chinese APT group starting early 2019. Starting then, over a span of five months, around 200 systems seem to have shown signs of having various tools associated with the investigated APT deployed within them. Some evidence suggests threat actors may have managed to compromise domain controllers from the victim's network, allowing them to move laterally and potentially gain control over a large number of machines from that infrastructure.

The investigation points to an attack meant to ensure persistence in the victims' network for as long as possible, to spy on victims by monitoring their activities and to exfiltrate intelligence.

ATTACK OVERVIEW

Discovery of a potential Chinese APT group targeting Southeast Asian governments using a sophisticated attack infrastructure that remains partially operational to this day.

Bitdefender presents the first detailed attack timeline and inventories the tools, techniques & procedures used by the APT group.

Presumed Objectives

- National security interests
- Industrial espionage
- Sensitive document retrieval

Target Selection

- Primarily Southeast Asian government institutions

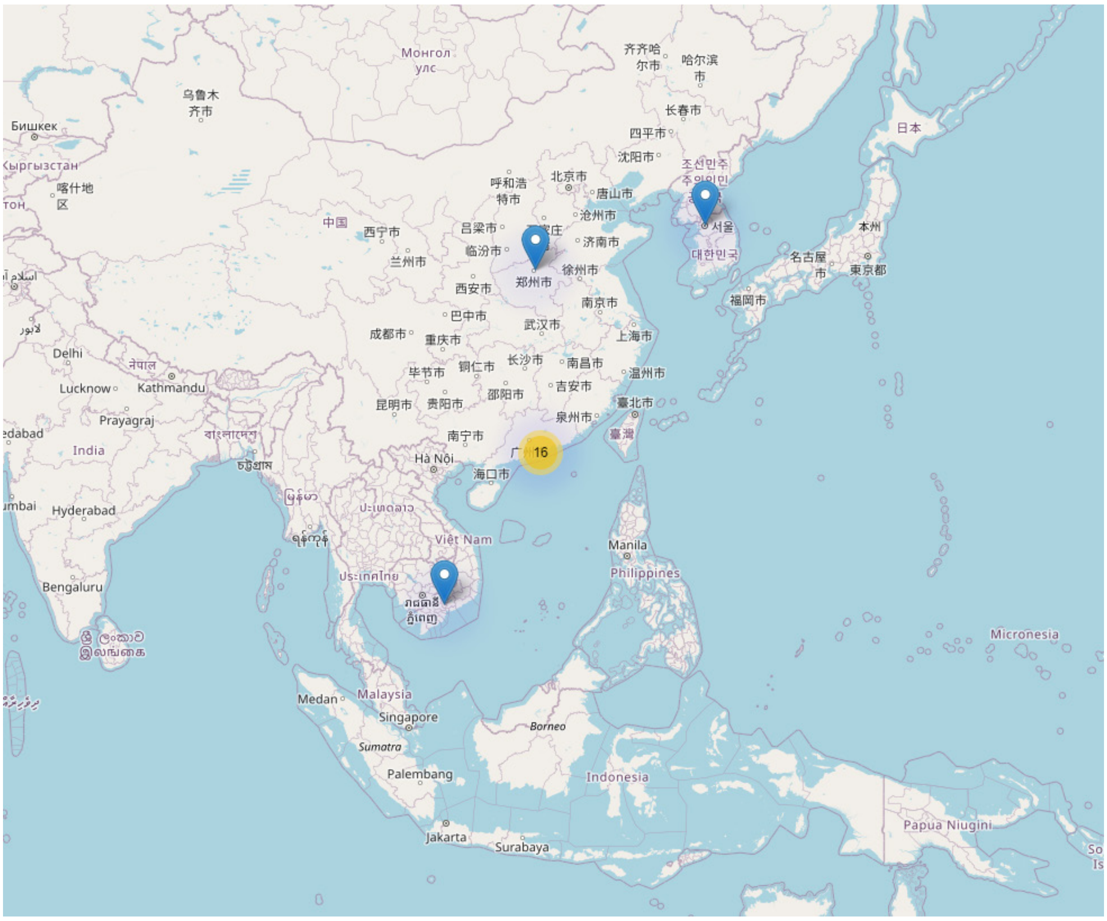
Exploit Tools and Techniques

- Persistence achieved via digitally signed binaries vulnerable to side-loading a backdoor into memory
- Extensive custom toolset designed for data exploration and exfiltration
- Three backdoors used for C&C: Chinoxy, PCShare, FunnyDream
- Potentially compromised domain controllers, gaining attacker control over the victim's network

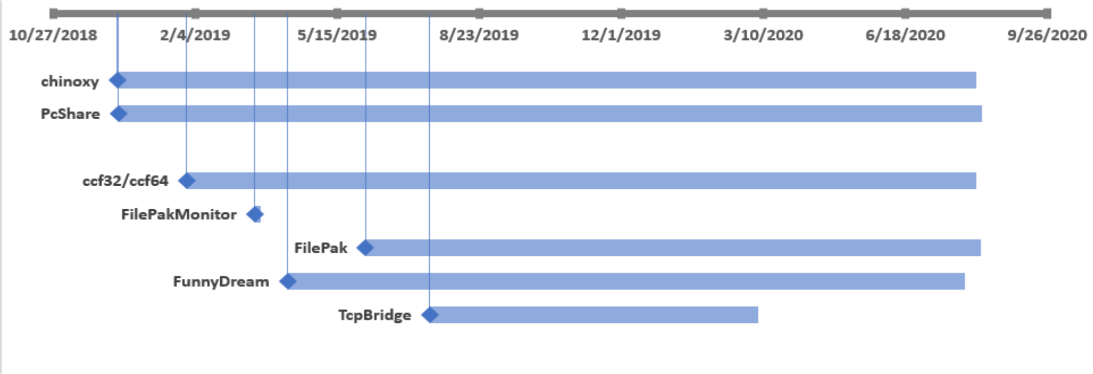
APT Campaign Reach

- Artifacts date from late-2018 and continue through 2020
- Over 200 machines showed attack indicators associated with this APT campaign
- Attack infrastructure likely continues to be active today

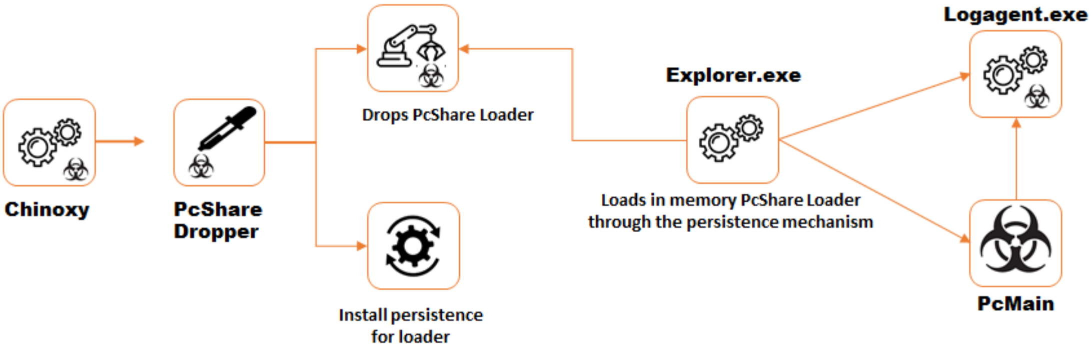
APT Command and Control Infrastructure Geolocation



APT Toolkit Usage Timeline



Installation of PcMain, the primary payload of the PCShare Remote Access Trojan


Chinoxy

PcShare Dropper

Drops PcShare Loader

Install persistence for loader

Explorer.exe

Loads in memory PcShare Loader through the persistence mechanism

Logagent.exe

PcMain

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security
NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test
SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row
More MSP-integrated solutions than any other security vendor
3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-ESDC_APT-DS-creat4927-en_EN
06/12/20November 5, 2020 1:19 pm11/05/20