SandWorm:

Russian State Hacker Group

By Jeffrey Farnan

TABLE OF CONTENTS

INTRODUCTION

Sandworm is a Russian state backed Russian Hacker Group which has been carry out cyberattacks in recent years. The Group is allegedly a Russian cyber military unit in charge of Russian military intelligence and has come under many different names such as Unit 74455, Telebots, Voodoo Bear, and Iron Viking. In this report we will look at cyberattacks attributed to Sandworm.

ABOUT SANDWORM

This report uncovers some of the first recorded instances of cyber warfare attributed to Russia's Main Intelligence Directorate or GRU. The elite hackers that make up this military unit are the definition of an advanced persistent threat (APT). This vastly resourced group, mainly targets Russia's neighbours such as Ukraine, Estonia, and Georgia.

-

The team is believed to be behind the December 2015 Ukraine power grid cyberattack, the 2017 cyberattacks on Ukraine using the Petya malware.

Although the indictment dates back to hacking activity five years ago, the Sandworm group has been linked to attempts to disrupt Ukrainian electrical power substations during the current conflict. Sandworm has previous as far as this is concerned, cutting power in Kiev back in 2016.

SANDWORM CYBERATTACKS

Some of the cyberattacks associated with Sandworm:

- NotPetya Malware
- Cyclops Blink
- VPNFilter
- ArguePatch Malware Loader
- Industroyer2
- CaddyWiper

SANDWORM HISTORY

The attacks employed in Sandworm's campaigns are often destructive, and the most notable are listed below:

- In December 2015 and December 2016, the Sandworm group executed cyberattacks against companies that support electric infrastructures, disrupting the supply of electricity to more than 225,000 Ukrainian customers.
- In 2017, Sandworm performed spearphishing waves that targeted local government, political parties and campaigns in France, including campaigns related to French President Emmanuel Macron's presidential campaign.
- In 2017 a notable malware campaign was launched – NotPetya – causing hundreds of victim organizations worldwide to lose $1 billion collectively. Petya and NotPetya are different malware variants, use different keys for encryption and have unique reboot styles, displays and notes. However, both are equally destructive.
- Sandworm launched attacks against the 2018 Winter Olympics after a Russian government-sponsored doping effort led to Russian athletes being unable to participate under the Russian flag.
- In October 2019, Sandworm defaced approximately 15,000 websites in Georgia.

CYCLOPS BLINK

Cyclops Blink is a new malware targeting network hardware with the goal of adding the targeted device to a botnet for command and control. This malware targets routers and firewall devices sold by the companies WatchGuard and ASUS. This malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and potentially destructive cyber-attack operations.

Cyclops Blink was first reported in February of 2022, after a number of security agencies disclosed its presents in the wild. It's designed to infect routers and other networked devices to steal data or compromise them for further attacks on other targets.

The US Justice Department has announced that the FBI has disrupted the Cyclops Blink botnet of thousands of infected network hardware devices. The FBI neutralized the threat before the slave computers could be weaponized.

- **Malware:** Cyclops Blink is a new malware targeting network hardware with the goad of adding the targeted device to a botnet for command and control (C&C). This malware targets routers and firewall devices sold by the companies WatchGuard and ASUS. These network devices are often located on the perimeter of a victim's computer network, thereby providing Sandworm with the potential ability to conduct malicious activities against all computers within those networks.

- **Malware Functionality:** The malware has basic core functionality to send information from the compromised device to a server controlled by the hackers, as well as allowing files to be downloaded and executed. The modules are specifically developed to upload/download files to and from its command and control server, collect device information, and update the malware. Additional functionality allows new modules to be added as the malware executes, causing Sandworm to add new features to an attack as needed.

- **Development:** The developers have reverse engineered the WatchGuard Firebox firmware update process and have identified a specific weakness in this process, namely the ability to recalculate the HMAC value used to verify a firmware update

image. They have taken advantage of this weakness to enable them to maintain the persistence of Cyclops Blink throughout the legitimate firmware update process.

- **Botnet:** The devices infected by Cyclops Blink have been incorporated into a large-scale botnet operated by the threat actor, which appears to have first become active as early as June 2019. Once established on targeted devices, the Cyclops Blink provides backdoor access to the compromised networks for the Sandworm hackers. The invasive features of the threat are spread through specifically designed modules. Some of the most notable harmful functions of the malware include the ability to fetch additional files, exfiltrated chosen files, collect and transmit device information and get updates from the operations of the Command-and-Control (C2) server. A significant amount of attention has been given to ensuring that the C2 communications are difficult to detect and track.

CADDYWIPER

CaddyWiper is a new wiper malware first discovered on March 14, 2020 in Ukraine. This wiper malware is specifically designed to damage target systems by erasing user data, programs, hard drives, and in some cases, partition information. As Russia's invasion of Ukraine continues, Threat Actors are infiltrating specific networks of organizations deemed high value before unleashing the wiper. Wipers are not focused on theft or financial gain -- but rather, they erase everything in their path for purely destructive purposes.

- CaddyWiper's primary purpose is to destroy user data and partition information for each available disk.
- The malware overwrites the main drive and any attached drives with null bytes which would corrupt them and destroy any stored data.
- It is smaller (compiled size of 9KB) than previous wipers attacks found in Ukraine, and has less complex capabilities than the others.

- When CaddyWiper is executed it first checks if the computer is a domain controller (DC). If the machine is a domain controller it does nothing. Stops execution.
- Try to gain admin privileges so has access to all files and folders on the system.
- It starts wiping files at "C:\\Users" so as not to break the operating system before the wiping process completes.
- When this stage is complete, the malware will attempt to access drives attached to the target system form "D:\\" to "Z:\\"
- Delete physical drive partitions to absolutely wreak the operating system.

.

DEFENSIVE MEASURES

Purely defensive measures will not prevent a Wiper attack. There are measures that will at least increase your odds of not being caught by this malware. Some recommendations include:

- Maintain up-to-date antivirus software
- Keep operating system patches up-to-date.
- Enable a personal firewall on workstations and configured to deny unsolicited connection requests.
- Regularly back up all important data, preferably offsite
- Harden all information systems to the greatest extent possible
- Recovery, response and business continuity plans should be tested and continuously tightened
- User and network segmentation
- Overlapping anti-malware solutions

WANTED BY THE FBI

The U.S. Department of Justice has charged six Russian intelligence operatives for hacking operations related to the Pyeongchang Winter Olympics, the 2017 French elections, and the notorious NotPetya Ransomware Attack.