Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage

By GReAT on February 9, 2016. 10:27 am

During the latter part of 2015, Kaspersky researchers from GReAT (Global Research and Analysis Team) got hold of the missing pieces of an intricate puzzle that points to the dawn of the first Portuguese-speaking targeted attack group, named “Poseidon.” The group’s campaigns appear to have been active since at least 2005, while the very first sample found points to 2001. This signals just how long ago the Poseidon threat actor was already working on its offensive framework.

Why has the Poseidon threat remained undetected for so many years? In reality, it has not. Most samples were detected promptly. However, Poseidon’s practice of being a ‘custom-tailored malware implants boutique’ kept security researchers from connecting different campaigns under the umbrella of a single threat actor. This approach entails crafting campaigns components on-demand and sometimes fabricating entirely unique malicious artifacts.

> 1st Portuguese-speaking group #ThePoseidonAPT attacks companies globally #TheSAS2016

Our research team was able to put together the disparate pieces of this puzzle by diligently tracing the evolution of Poseidon’s toolkit in pursuit of an overarching understanding of how the actor thinks and the specific practices involved in infecting and extorting its victims. With a set of tools developed for the sole purpose of information gathering and privilege escalation, the sophistication level of campaign highlights that, today, regional actors are not far behind better-known players in the global game of targeted attacks.

Becoming familiar with the operations of the Poseidon Group meant patiently dismantling their modus operandi to unearth the custom-designed infection tools deployed to each of their selected targets. This process revealed a series of campaigns with highly-regionalized malware practices and geographically-skewed victim tasking, unsurprising in a region with a gradually-maturing cybercrime industry. The proper detection of each iteration of their evolving toolkit may have been enough to thwart specific efforts, but to truly understand the magnitude of Poseidon’s combined operations required an archeological effort to match.

Frequently asked questions

What exactly is the Poseidon Group?

The Poseidon Group is a long-running team operating on all domains: land, air, and sea. They are dedicated to running targeted attacks campaigns to aggressively collect information from company networks through the use of spear-phishing packaged with embedded, executable elements inside office documents and extensive lateral movement tools. The information exfiltrated is then leveraged by a company front to blackmail victim companies into contracting the Poseidon Group as a security firm. Even when contracted, the Poseidon Group may continue its infection or initiate another infection at a later time, persisting on the network to continue data collection beyond its contractual obligation. The Poseidon Group has been active, using custom code and evolving their toolkit since at least 2005. Their tools are consistently designed to function on English and Portuguese systems spanning the gamut of Windows OS, and their exfiltration methods include the use of hijacked satellite connections. Poseidon continues to be active at this time.

Why do you call it Poseidon's Targeted Attack Boutique?

The presence of several text fragments found in the strings section of executable files belonging to the campaign reveal the actor's fondness for Greek mythology, especially regarding Poseidon, the God of the Seas (which also coincides with their later abuse of satellite communications meant to service ships at sea). The boutique element is reflected in their artisanally adaptive toolkit for lateral movement and data collection which appears to change from infection to infection to fit custom-tailored requirements for each of their prospective clients. The business cycle includes what is euphemistically referred to as 'financial forecasting' using stolen information, so we like to say that Poseidon's boutique not only deals in targeted attacks but also stolen treasures.

How did you become aware of this threat? Who reported it?

We noticed that several security companies and enthusiasts had unwittingly reported on fragments of Poseidon's campaigns over the years. However, nobody noticed that these fragments actually belonged to the same threat actor. Perhaps because many of these campaigns were designed to run on specific machines, using English and Portuguese languages, with diverse command and control servers located in different countries and soon discarded, signing malware with different certificates issued in the name of rogue companies, and so on. By carefully collecting all the evidence and then reconstructing the attacker's timeline, we found that it was actually a single group operating since at least 2005, and possible earlier, and still active on the market.

With this understanding, GReAT researchers were able to recognize similarities in obfuscation and development traits leading back to widely-reported but little understood variants on a sample in 2015, which searched for prominent leaders and secret documents involving them.

When did you discover this targeted attack?

The very first samples from this campaign were detected by Kaspersky Lab back in the early 2000s. However, as noted previously, it is a very complex task to correlate indicators and evidence in order to put together all the pieces of this intricate puzzle. By the middle of 2015 it was possible to identify that throughout this period of time it's been the same threat actor, which we call Poseidon Group.

Who are the victims? / What can you say about the targets of the attacks?

The targets are companies in energy and utilities, telecommunications, public relations, media, financial institutions, governmental institutions, services in general and manufacturing. The geographical spread of victims is heavily-skewed towards Brazil, the United States, France, Kazakhstan, United Arab Emirates, India and Russia. Many of the victims have joint ventures or partner operations in Brazil. The importance of the victims is not measured in numbers since each of these victims is a large-scale (often multinational) enterprise.

What exactly is being stolen from the target machines?

One of the characteristics of the group behind Poseidon is an active exploration of domain-based networks. Such network topology is typical for companies and enterprises.

The highest value asset for these companies is proprietary information, technologies, and business-sensitive information that represents significant value in relation to investments and stock valuations. The Poseidon Group actively targets this sort of corporate environment for the theft of intellectual property and commercial information, occasionally focusing on personal information on executives.

How does Poseidon's APT Boutique infect computers?

The main infection vector for Poseidon is the use of spear-phishing emails including RTF/DOC files, usually with a human resources lure. The executables are also often digitally signed and occasionally hidden in alternate data streams to fool security solutions. Poseidon's toolkit displays an awareness of many antivirus providers over the years, attempting to attack or spoof these processes as a means of self-defense for their infections. Once the infection happens, it reports to the command and control servers before beginning a complex lateral movement phase. This phase will often leverage a specialized tool that automatically collects a wide array of information including credentials, group management policies, and even system logs to better hone further attacks and assure execution of their malware. This way the attackers actually know what applications and commands they can use without raising an alert to the network administrator during lateral movement and exfiltration.

What does the Poseidon Group do? What happens after a target machine is infected?

Once the target's machine is compromised, the attacker first enumerates all processes running in the system and all services. Then the attacker looks for all administrator accounts on both the local machine and the network. This technique allows them to map network resources and make lateral movements inside the network, landing in the perfect machine to match the attacker's interest. This reflects the Poseidon Group's familiarity with Windows network administration. In many cases, their ultimate interest is the Domain Controller.

Additionally malware reports itself to its hardcoded command and control servers and established a backdoor connection, so the attacker may have a permanent remote connection.

What are the malicious tools used by the Poseidon Group? What are their functions?

Poseidon utilizes a variety of tools. Their main infection tool has been steadily evolving since 2005, with code remnants remaining the same to this day, while others have been altered to fit the requirements of new operating systems and specific campaigns. A noteworthy addition to the Poseidon toolkit is the IGT supertool (Information Gathering toolkit), a bulking 15 megabyte executable that orchestrates a series of different information collections steps, exfiltration, and the cleanup of components. This tool appears to be designed to operate on high-value corporate systems like Domain Controllers or IIS servers that act as repositories of valuable information, particularly for lateral movement. The Information Gathering Tool (IGT) tool is coded in Delphi and includes powershell and SQL components across a dozen different drops. This tool contains several other executable files made in different programming languages ranging from Visual Basic 6 to C#, each one performing a very clear task devised by the group when trying to obtain more information from an objective. The main purpose of the IGT tool is to make an inventory of the system, saving information from the network interfaces and addresses, credentials belonging to the Domain and database server, services being run from the OS and everything that could help the Poseidon Group make its attack more customized to its victim.

Are the attackers using any zero-day vulnerabilities?

No zero-day vulnerabilities have been found in the analysis of the samples obtained regarding this campaign. Poseidon's conventional means of deceiving users with executable files posing inside Word and RTF document files, and actual poisoned documents with malicious macro-scripts has been the sole method used for compromising their desired targets. As we have seen in other targeted campaigns, social engineering and carefully crafted spear-phishing attacks play a crucial role in the effectiveness of getting a foothold in the desired system.

Is this a Windows-only threat? Which versions of Windows are targeted?

Poseidon is particularly focused on the Microsoft Windows operating system family, specifically customizing the infection method for each one so as to gather different information and hide its presence after the initial infection. Other products usually found in corporate environments, such as an SQL server, are being used for lateral movement and credential harvesting using a customized toolset designed by the crafty Poseidon Group. Because of Poseidon's longevity, there are samples targeting Windows systems as early as Windows NT 4.0 Server and Windows 95 Workstation up to current versions like Windows 8.1, as well as server variants (very important to them, given the emphasis on reaching Domain Controllers in corporate environments.)

How is this different from any other targeted attack?

The extortion elements of this campaign are what set it apart from others. The exfiltration of sensitive data is done in order to coerce the victim into a business relationship under the threat of exchanging this information with competitors or leveraging it as part of the company's offering of 'investment forecasting'. Additionally this is the first ever publicly known Portuguese-speaking targeted attacks campaign.

Are there multiple variants of the Poseidon Group’s malware? Are there any major differences in the variants?

Poseidon has maintained a consistently evolving toolkit since the mid-2000s. The malware has not avoided detection but instead been so inconspicuous as to not arouse much suspicion due to the fact that this malware only represents the initial phase of the attack. An altogether different component is leveraged once Poseidon reaches an important machine like an enterprise’s Domain Controller. This is where the main collection takes place by use of the IGT (Information Gathering Tool) toolkit.

Is the command and control server used by the Poseidon Group still active? Have you been able to sinkhole any of the command and controls?

Poseidon Group has interesting practices when it comes to its use of command and control servers, including redundancies and quickly discarding command and control (C&Cs) servers after specific campaigns. This has actually allowed us to sinkhole several domains. A few of these still had active infections attempting to report to the C&Cs. This adds an interesting dimension to the story. As part of Kaspersky Lab’s commitment to securing cyberspace for everyone, we reached out and notified identifiable victims, regardless of their security solution and provided them with indicators of compromise (IOCs) to help root out the active infection. In the process, we were able to confirm the previously described operating procedures for the Poseidon Group.

Is this a state-sponsored attack? Who is responsible?

We do not believe this to be a state-sponsored attack but rather a commercial threat player. Collaboration with information-sharing partners and victim institutions allowed us to become aware of the more complicated business cycle involved in this story, greatly adding to our research interest in tracking these campaigns. The malware is designed to function specifically on English and Portuguese-language systems. This is the first ever Portuguese-speaking targeted attack campaign.

How long have the attackers been active?

The attackers have been active for more than ten years. The main distribution of samples goes back to 2005 with possible earlier outliers.

Operating systems such as Windows 95 for desktop computers and Windows NT for server editions were not uncommon at the time and Poseidon’s team has evolved gradually into targeting the latest flagship editions of Microsoft’s operating systems. Recent samples show interest in Windows 2012 Server and Windows 8.1.

Did the attackers use any interesting/advanced technologies?

During a particular campaign, conventional Poseidon samples were directed to IPs resolving to satellite uplinks. The networks abused were designed for internet communications with ships at sea which span a greater geographical area at nearly global scale, while providing nearly no security for their downlinks.

The malware authors also possess an interesting understanding of execution policies which they leverage to manipulate their victim systems. They combine reconnaissance of GPO (Group Policy Object management for execution) with digitally-signed malware to avoid detection or blocking during their infection phases. These digital certificates are often issued in the name of rogue and legitimate companies to avoid arousing suspicion from researchers and incident responders.

Does Kaspersky Lab detect all variants of this malware?

Yes, all samples are detected by signatures and also heuristics. With a fully updated Kaspersky Lab anti-malware solution, all customers are protected now. Kaspersky Lab products detect the malware used by Poseidon Group with the following detection names:

Backdoor.Win32.Nhopro
HEUR:Backdoor.Win32.Nhopro.gen
HEUR:Hacktool.Win32.Nhopro.gen

How many victims have you found?

At least 35 victim companies have been identified with primary targets including financial and government institutions, telecommunications, manufacturing, energy and other service utility companies, as well as media and public relations firms.

The archaeological effort of understanding such a long-standing group can severely complicate victim identification. We see traces of upwards of a few tens of companies targeted. The exact number of the victims may actually vary. Since it is a very long term group, some victims may be impossible to identify now.

At this time, we are reaching out to victims of active infections to offer remediation assistance, IOCs, and our full intelligence report to help them counteract this threat. Any victims or potential targets concerned about this threat should please contact us at intelreports@kaspersky.com.

Who is behind these attacks?

We do not speculate on attribution. Language code used to compile implants, as well as the language used to describe certain commands used by the group, actually corresponds to Portuguese from Brazil. The inclusion of Portuguese language strings and preference for Portuguese systems is prominent throughout the samples.

The tasking of Poseidon’s campaigns appears to be heavily focused on espionage for commercial interests. Speculating further would be unsubstantiated.

Reference samples hashes:

2ce818518ca5fd03cbacb26173aa60ce
f3499a9d9ce3de5dc10de3d7831d0938
0a870c900e6db25a0e0a65b8545656d4

2fd8bb121a048e7c9e29040f9a9a6eee

4cc1b23daaaac6bf94f99f309854ea10

2c4aeacd3f7b587c599c2c4b5c1475da

f821eb4be9840feaf77983eb7d55e5f6

2ce818518ca5fd03cbacb26173aa60ce

Command and control servers:

akamaihub[.]com – SINKHOLED by Kaspersky Lab
igdata[.]net – SINKHOLED by Kaspersky Lab
mozillacdn[.]com – SINKHOLED by Kaspersky Lab
msupdatecdn[.]com – SINKHOLED by Kaspersky Lab
sslverification[.]net – SINKHOLED by Kaspersky Lab

For more about counter Poseidon and similar attacks, read this article in the Kaspersky Business Blog.