A Touch of Artistry: Poseidon’s APT Boutique

Feb 9, 2016 Oleg Gorobets Featured Post, Technology, Threats No comments

Targeted attacks are visibly commoditizing, choosing cost efficiency over sophistication. If a combination of social engineering, tweaks to widely-available malware and legit apps can do the trick, why bother to create something original and exquisite?

Nevertheless there remain true adepts – those who perceive every cyberespionage operation as another stage in the quest for ultimate perfection. And, given the long and successful careers of some, they have good reason to stick with their own way of working.

Artistic Blackmailers

The Poseidon cyberespionage group very much fits this description. The group has been using state-of-the-art custom malware since 2005, at least, and there's data to suggest that some could have been prototyped as early as 2001. Different components of their toolsets appeared regularly on the radar of security companies, but were not recognized as part of a bigger picture. Throughout this period, Poseidon were meticulously tailoring their toolsets to ensure easy and silent entry and efficient data acquisition, in line with their patrons' requirements. This perfectionist, artisan approach, together with the group's known fascination with Greek mythology and their one-time abuse of a maritime satellite communications system, earned their operations the nickname 'Poseidon's APT Boutique'.

> *A Touch of Artistry: Poseidon's APT Boutique #PoseidonAPT*
>
> Tweet

Setting aside their artistic finesse, some aspects of their 'business model' looked distinctly ugly. Masquerading behind a front-end 'security company', they used harvested secrets to blackmail targets into accepting them as IT security contractors. Meanwhile, they either retained an illegitimate presence within the 'secured' system or, having completed the task agreed, quietly resumed their presence within the perimeter. They were known to refer to one element their business cycle as

‘financial forcasting’, giving an idea of the long-term benefit they anticipated from a prolonged systems presence. With their focus on Windows-based systems and extremely developed skills, they could theoretically embed themselves within the victim’s IT system for years without being detected.

Great Art Demands Sacrifices

The Poseidon’s targets have tended to be large Enterprises, mainly centering round Brazil, the US, France, Kazakhstan and Russia. There appears an interesting language limitation to English and Brazilian Portuguese based systems: even in countries with different national languages, the IT networks of multi-national corporations having these locales and/or keyboard layouts were preferred as targets. Their sphere of interest has encompassed Energy and Utilities, Manufacturing – and also Media and PR. The latter two could obviously provide attackers with plenty of information for use as ammunition against additional future targets.

> *The Poseidon’s targets have tended to be large Enterprises #PoseidonAPT*

Tweet

Tools of the Artisan’s Trade

To many an artisan eye, elegance and simplicity go hand by hand. The Poseidon group seem to embrace this principle. For initial penetration, they use no exploits; only well-crafted spear-phishing

emails carrying DOC/RTF files with encapsulated executables – an uncommon approach nowadays. To fool existing security solutions, they often sign these binaries with real certificates – issued for fake companies or even belonging to genuine well-respected and trusted organizations. Having successfully infecting their first victims, the collection of extensive data about the attacked infrastructure begins. Using this information, and ace Windows admin skills, the attackers can then move laterally without triggering any alarms, their next objective being to obtain Domain Admin rights. With this level of power, they can then purge the majority of their own tools from the network, retaining only those essential to their ongoing presence and data exfiltration.

As already mentioned, in one series of operations Poseidon used ships' satellite communication systems as hiding places for their Command & Control (C&C) servers, a similar mechanism to that used by the Turla actor. No attempts to repeat this feat have, however, been recorded.

What Can Be Done?

Despite all Poseidon's attempts to disguise and disperse the evidence, experts from Kaspersky Lab's Global Research and Analysis Team have succeeded in piecing all the disparate pieces of data into a complete picture. Still, the Poseidon group remains active, which brings us to the question of adequate defense.

Of course protecting endpoints is a must – which, as the well-known ASD Mitigation Strategies suggest, should comprise non-signature detection mechanisms, such as Heuristics and Behavioral Detection Algorithms. Possessing all these, Kaspersky Endpoint Security for Business is powered by the same superior Security Intelligence that enabled our experts to piece together the previously insoluble Poseidon puzzle. Kaspersky Endpoint Security for Business also provides further proactive

security layers – including Security Controls, HIPS and a built-in Application Firewall – all fed by real-time global intelligence from the Kaspersky Security Network. These layers erect further barriers in the path of malware, from blocking launch attempts to preventing access to critical system elements and communications with C&C.

The extent of information harvesting by the Poseidon group also highlights the benefits of Data Encryption throughout the whole corporate infrastructure, enforced by appropriate policies. The Advanced tier of Kaspersky Endpoint Security for Business includes easy-to-use Encryption Technology, managed through the same single-pane-of-glass console of Kaspersky Security Center as all platform elements. Of course, with spear-phishing as the penetration method of choice for the majority of Targated Attack groups, scanning email streams is also absolutely crucial nowadays. Kaspersky Security for Mail Servers erects another powerful defensive wall in the attacker's way.

All in all, Kaspersky Lab's portfolio of solutions helps implement 19 of ASD's 35 Mitigation Strategies, including 3 of the 'top 4' which between them prevent 85% Targeted Attack-related incidents. But even if you use another vendor's solutions to protect your infrastructure, we can help. Kaspersky Lab's achievements as APT discoverers demonstrate that the presence even of such a stealthy and capable APT actor as Poseidon can be uncovered; that's what our Targeted Attack Discovery service is for[1].

Secrets are worth most when they're sold red hot. Perhaps it's time to prevent your organization from getting burned.

For more about the Poseidon's APT Boutique, read the following blogpost on Securelist.

Kaspersky Lab products detect Poseidon malware under the following verdicts:

Backdoor.Win32.Nhopro

HEUR:Backdoor.Win32.Nhopro.gen

HEUR:Hacktool.Win32.Nhopro.gen

[1] Available only in a limited number of regions. To find out whether this is available in your region, please contact Kaspersky Lab manager.

PoseidonAPT TheSAS2016

About Oleg Gorobets

Technology Positioning Group Manager, Kaspersky Lab

View all posts by Oleg Gorobets →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

I'm not a robot

reCAPTCHA

Post Comment

Related Posts

The wind that smells like RAT: The story of Adwind MaaS

Feb 8, 2016

Bank Busting and Beyond: Metel, GCMan and Carbanak 2.0!

Feb 8, 2016

Welcome to Kaspersky Security Analyst Summit 2016!

Feb 8, 2016

Kaspersky Security Analyst Summit: a few words about training

Nov 24, 2015

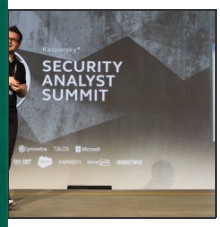
Popular Posts

1 Introducing Kaspersky Lab DDoS Datasheet

Nov 19, 2015 1

2 Smart City security: is it time to start worrying?...

Industry News



Vitaly Kamluk on the Adwind RAT

Chris Brook

February 9, 2016

Medical Device, Health Care Security Continues to Ail

Michael Mimoso

February 9, 2016

Power Grid Honeypot Puts Face on Attacks

Michael Mimoso

February 9, 2016

Poseidon APT Group Identified As First Portuguese-Speak...

Chris Brook

February 9, 2016

Dec 3, 2015 1

3 Hyatt hotel chain hit by financial malware; how to...
Jan 27, 2016 0

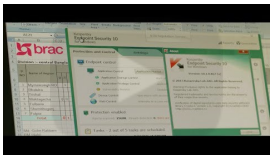
4 Kaspersky Lab vs world poverty: a case study
Jan 22, 2016 0

5 An hostile ear in your pocket: how cyberspies may ...
Jan 20, 2016 0

IoT's Day of Reckoning on the Horizon
Chris Brook
February 8, 2016

Latest Videos





This week we talk about

#banking 1 #EnterpriseSec 5

0day 3

2014 cyberthreats statistics 1

2015 2 2016 2

451 Research 1 911 1

February 2016

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29						

« Jan

Contributors

AAA ratings 1

Adobe 3

Time Machine

February 2016

January 2016

December 2015

November 2015

October 2015

September 2015

August 2015

July 2015

June 2015

May 2015

April 2015

March 2015

February 2015

January 2015

December 2014

November 2014

October 2014

September 2014

August 2014

July 2014

June 2014

May 2014

April 2014

March 2014

February 2014

January 2014

December 2013

November 2013

October 2013

September 2013

Yuri Ilyin

325 posts

Konstantin Goncharov

44 posts

Oleg Gorobets

8 posts

Cynthia James

8 posts

Denis Makrushin

7 posts

August 2013

July 2013

June 2013

May 2013

April 2013

Tag Cloud

Android Apple APT big data
Business News Business Security
byod corporate security
cryptolocker cybercriminals
Cyber Espionage CyberSecurity
cyberthreats data encryption
data leaks data security DDoS
encryption endpoint security fraud
heartbleed IT IT security
IT threats
kaspersky endpoint security
Kaspersky Lab
Kaspersky Small Office Security
malware Microsoft mobile device
patches phishing protectmybiz
ransomware security
Security for Very Small Businesses
security news shellshock spam
survey thesas2015
threat landscape threats
vulnerabilities Windows

Propose a Topic

Name

Email

Message

Send

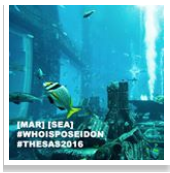
Topics

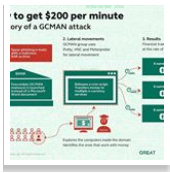
Android | Apple | APT | big data | Business News | Business Security | byod | corporate security | cryptolocker | cybercriminals | Cyber Espionage | CyberSecurity | cyberthreats | data encryption | data leaks | data security | DDoS | encryption | endpoint security | fraud | heartbleed | IT | IT security | IT threats | kaspersky endpoint security | Kaspersky Lab | Kaspersky Small Office Security | malware | Microsoft | mobile device | patches | phishing | protectmybiz | ransomware | security | Security for Very Small Businesses | security news | shellshock | spam | survey | thesas2015 | threat landscape | threats | vulnerabilities | Windows

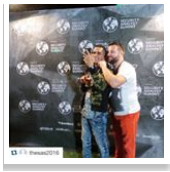
Instagram



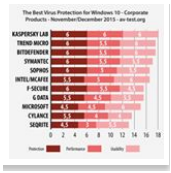











Subscribe to RSS Feeds

Get all latest content delivered to your email a few times a month.

Your email

Sign Up

Products for Home

- Kaspersky PURE 3.0
- Kaspersky Internet Security–Multi-Device
- Kaspersky Internet Security 2015
- Kaspersky Anti-Virus 2015
- Kaspersky Internet Security for Mac
- Kaspersky Internet Security for Android
- Kaspersky Password Manager
- Kaspersky Security Scan FREE

Products for Enterprise Business

- Kaspersky Endpoint Security for Business | Advanced
- Kaspersky Endpoint Security for Business | Select
- Kaspersky Endpoint Security for Business | Core
- Kaspersky Total Security for Business
- Targeted Security Solutions

Products for Small Office

- Kaspersky Small Office Security

For Software Users

- Buy online
- Renew license
- Get updates
- Try for free

Technical Support

- For home products
- For business products

About Us

- About Kaspersky Lab

Blogroll

39A/3 Leningradskoe shosse
Moscow
125212
Russia