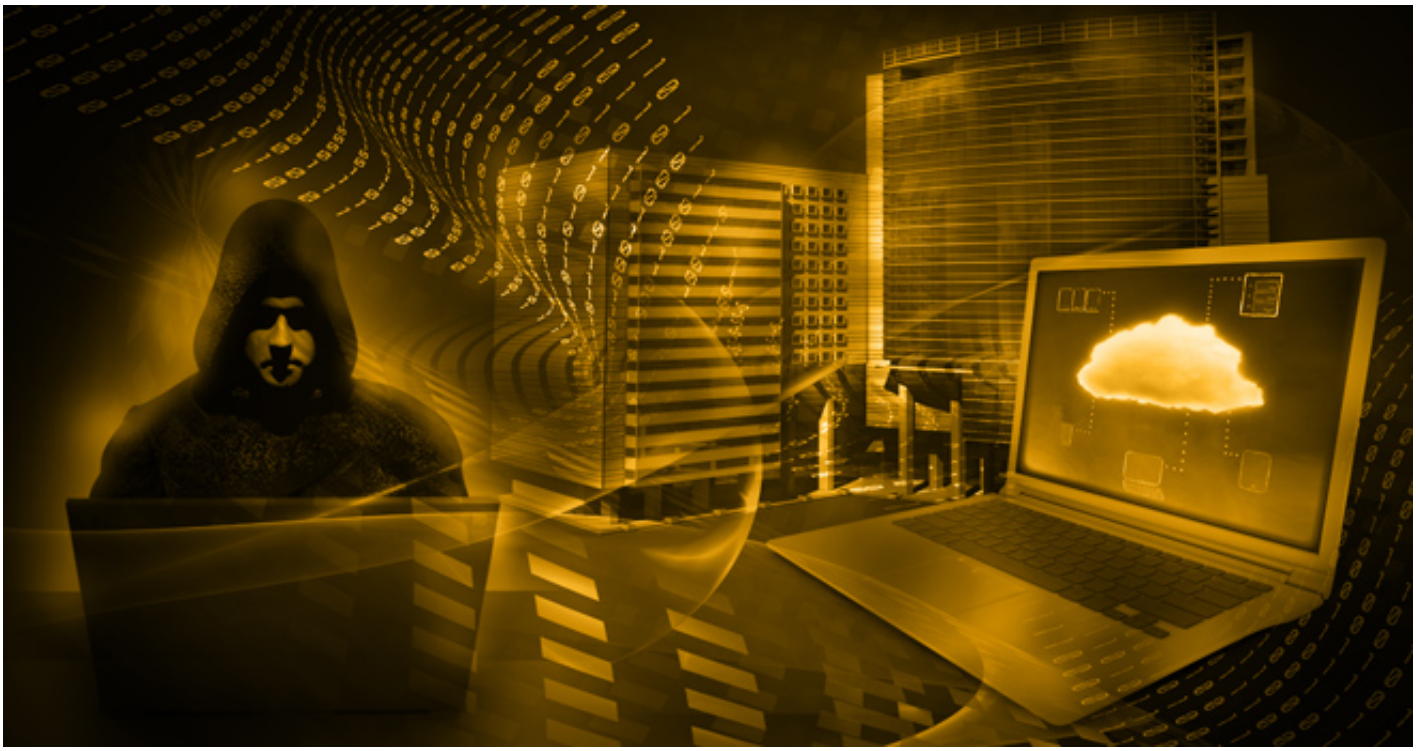
"Forkmeiamfamous": Seaduke, latest weapon in the Duke armory

Low-profile information-stealing Trojan is used only against high-value targets.



Symantec has uncovered an elusive Trojan used by the cyberespionage group behind the â€œDukeâ€ family of malware. Seaduke (detected by Symantec as Trojan.Seaduke) is a low-profile information-stealing Trojan which appears to be reserved for attacks against a small number of high-value targets.

Seaduke has been used in attacks against a number of major, government-level targets. The malware hides behind numerous layers of encryption and obfuscation and is capable of quietly stealing and exfiltrating sensitive information such as email from the victimâ€™s computer. Seaduke has a highly configurable framework and Symantec has already found hundreds of different configurations on compromised networks. Its creators are likely to have spent a considerable amount of time and resources in preparing these attacks and the malware has been deployed against a number of high-level government targets.

While the Duke group began to distribute Cozyduke in an increasingly aggressive manner, Seaduke installations were reserved only for select targets. Seaduke victims are generally first infected with Cozyduke and, if the computer appears to be a target of interest, the operators will install Seaduke.

Background
The group behind Seaduke is a cyberespionage operation that is responsible for a series of attacks against high-profile individuals and organizations in government, international policy and private research in the United States and Europe. It has a range of malware tools at its disposal, known as the Dukes, including Cozyduke (Trojan.Cozer), Miniduke (Backdoor.Miniduke) and Cosmicduke (Backdoor.Tinybaron).

News of the Duke group first emerged in March and April of 2015, when reports detailing attacks involving a sophisticated threat actor variously called Office Monkeys, EuroAPT, Cozy Bear, and Cozyduke were published. Symantec believes that this group has a history of compromising governmental and diplomatic organizations since at least 2010.

The group began its current campaign as early as March 2014, when Trojan.Cozer (aka Cozyduke) was identified on the network of a private research institute in Washington, D.C. In the months that followed, the Duke group began to target victims with â€œOffice Monkeysâ€- and â€œeFaxâ€-themed emails, booby-trapped with a Cozyduke payload. These tactics were atypical of a cyberespionage group. Itâ€™s quite likely these themes were deliberately chosen to act as a smokescreen, hiding the true intent of the adversary.

Figure 1. Cozyduke campaign used an â€œOffice Monkeysâ€ video as a lureâ€“July 2014

The Duke group has mounted an extended campaign targeting high-profile networks over extended periods, something which is far beyond the reach of the majority of threat actors. Its capabilities include:

- Attack infrastructure leveraging hundreds of compromised websites
- Rapidly developed malware frameworks in concurrent use
- Sophisticated operators with fine-tuned computer network exploitation (CNE) skills

Although Cozyduke activity was first identified in March 2014, it wasnâ€™t until July that the group managed to successfully compromise high-profile government networks. Cozyduke was used throughout these attacks to harvest and exfiltrate sensitive information to the attackers.

In parallel, the Duke group was also installing separate malware onto these networks, namely Backdoor.Miniduke and the more elusive Trojan.Seaduke. It could use these payloads to exploit networks on multiple fronts and providing it with additional persistence mechanisms.

The Miniduke payload

In July of 2014, the group instructed Cozyduke-infected computers to install Backdoor.Miniduke onto a compromised network. Miniduke has been the groupâ€™s tool of choice for a number of years in espionage operations predominantly targeting government and diplomatic entities in Eastern Europe and ex-Soviet states. â€œNemesis Geminaâ€ appears to be the internal name for the framework used by the group to identify the project, previously reported by Kaspersky.

The following debug string was present in the sample used in these attacks:

- C:\Projects\nemesis-gemina\nemesis\bin\carriers\ezlzma_x86_exe.pdb

This project name has been seen in Backdoor.Tinybaron (aka Cosmicduke) samples, which Symantec also attributes to the Duke group. This deployment of Miniduke and the technical similarities with Cozyduke provided strong indicators as to who was behind the attacks.

The Seaduke payload
These attacks were already well underway when another group began to deploy a previously unknown piece of malware. In October 2014, the Seaduke payload began to appear within target networks. Although Seaduke was developed in Python, the overall framework bears a striking resemblance to Cozyduke in terms of operation. Itâ€™s unclear why the attackers waited until October to deploy Seaduke. Was it reserved for a more specific attack? Was part of their cover blown, necessitating the use of an alternative framework?

The Seaduke framework was designed to be highly configurable. Hundreds of reconfigurations were identified on compromised networks. The communication protocol employed had many layers of encryption and obfuscation, using over 200 compromised web servers for command and control. Seaduke required a significant investment of time and resources in the preparatory and operational phases of the attack.

Seaduke delivery
The attackers control Cozyduke via compromised websites, issuing instructions to infected machines by uploading â€œtasksâ€ to a database file. Cozyduke will periodically contact these websites to retrieve task information to be executed on the local machine. One such task (an encoded PowerShell script) instructed Cozyduke to download and execute Seaduke from a compromised website.

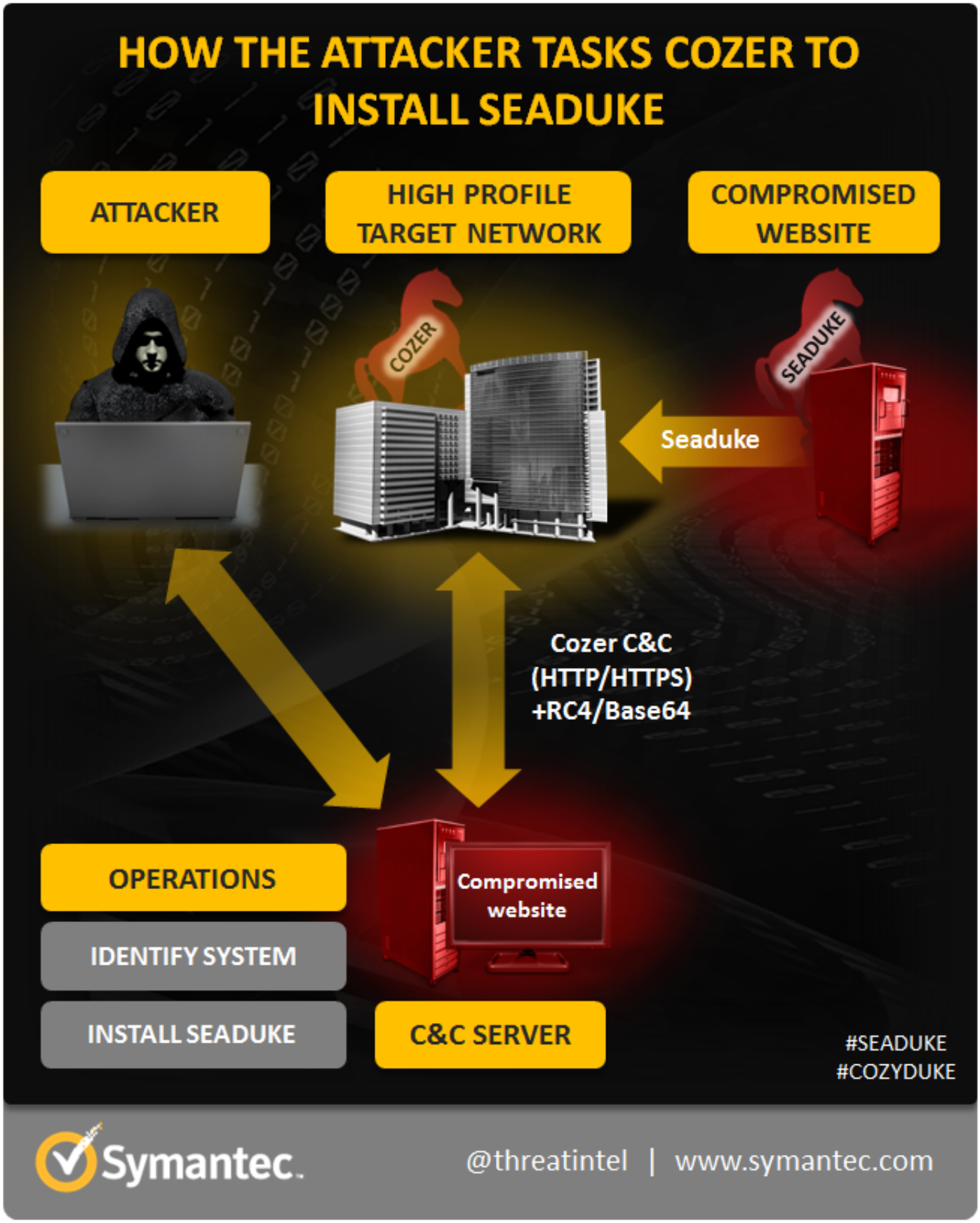


Figure 2. How the attacker tasks Cozer to install Seaduke

Seaduke operation

The attackers can operate Seaduke in a broadly similar fashion to Cozyduke. The Seaduke control infrastructure is essentially distinct, opening up the possibility of sub-teams concurrently exploiting the

target network. Unlike Cozyduke, Seaduke operators upload â€œtaskâ€ files directly to the command-and-control (C&C) server; there is no database as such present. Seaduke securely communicates with the C&C server over HTTP/HTTPS beneath layers of encoding (Base64) and encryption (RC4, AES). To an untrained eye, the communications look fairly benign, no doubt an effort to stay under the radar on compromised networks.

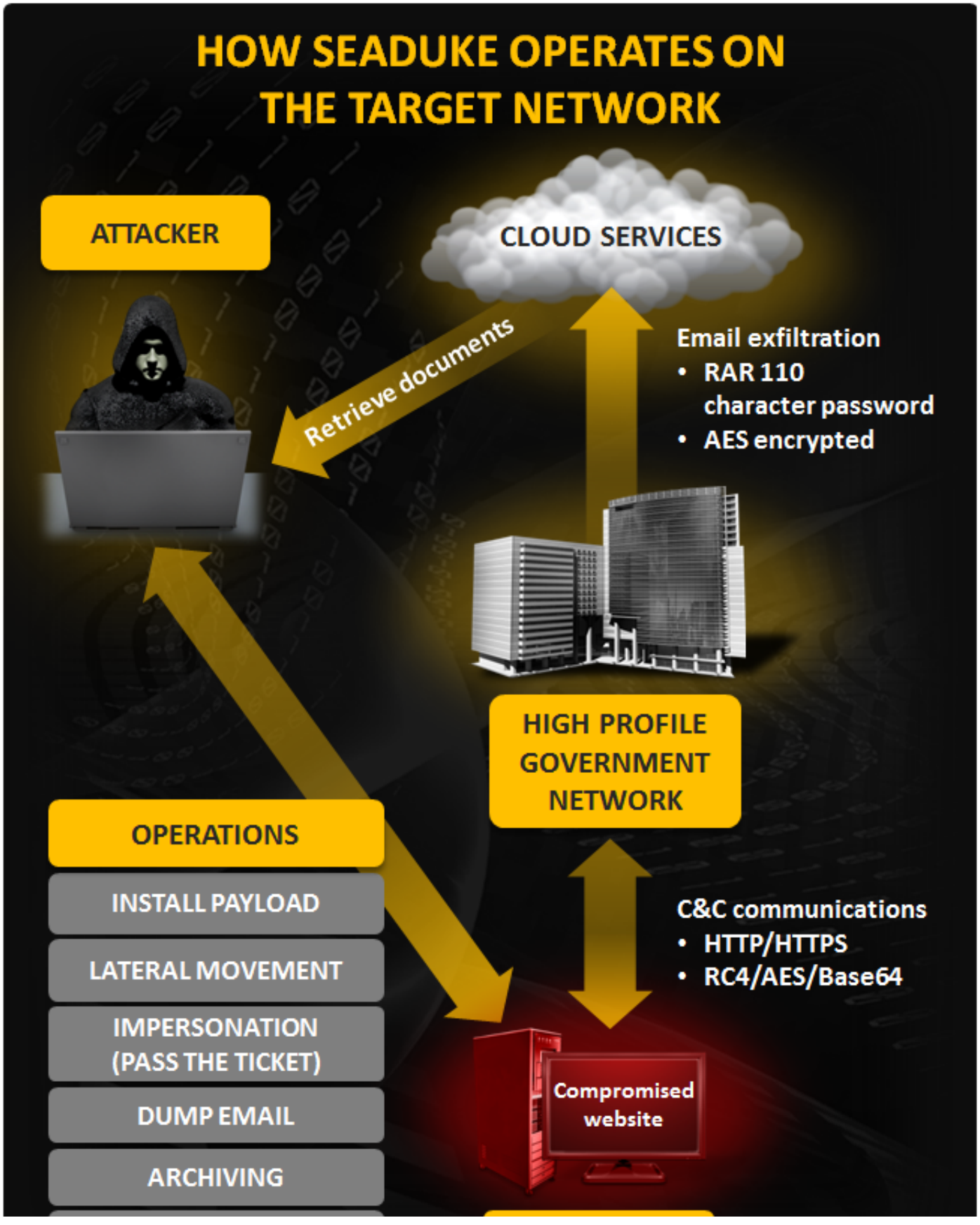


Figure 3. How Seaduke operates on the target network

Seaduke has many inbuilt commands which are available to the attackers. They have the ability to retrieve detailed bot/system information, update bot configuration, upload files, download files, and self-delete the malware from the system. The self-delete function is interestingly called â€œseppukuâ€. This is a form of Japanese ritual suicide.

Seaduke payloads

The attackers have also developed a number of additional payloads. Operators can push these payloads onto infected machines for very specific attacks.

- Impersonation using Kerberos pass-the-ticket attacks (Mimikatz PowerShell)
- Email extraction from the MS Exchange Server using compromised credentials
- Archiving sensitive information
- Data exfiltration via legitimate cloud services
- Secure file deletion

What next?

The Duke group has brought its operational capability to the next level. Its attacks have been so bold and aggressive, that a huge amount of attention has been drawn to it, yet it appears to be unperturbed. Its success at compromising such high-profile targets has no doubt added a few feathers to its cap. Even the developers reveled in this fact, naming one of Seadukeâ€™s functions â€œforkmeiamfamousâ€.

While the group is currently keeping a lower profile, thereâ€™s no doubt it will reappear. Some tools may have to be abandoned, some reworked and others built completely from scratch. This attack group is in it for the long haul.