ENSILO
SILO YOUR DATA FROM THREAT ACTORS

MENU

OCTOBER 6, 2015 BY YOTAM GOTTESMAN

Moker: A new APT discovered within a sensitive network

Recently, enSilo found an Advanced Persistent Threat (APT) residing in a sensitive network of a customer. This APT appears to be a Remote Access Trojan (RAT) that is capable of taking complete control of the victim's computer.

To date, this APT is unknown and does not appear in VirusTotal.

Moker was the file description that the malware author gave to the malware's executable file.

enSilo's customers are all safeguarded from Moker.

What makes Moker unique?

- **Bypasses and disables security measures**. This includes everything from security-dedicated measures such as Anti-Virus (AV), sandboxing and virtual machines, to Windows' built-in security enhancements such as User Access Control (UAC).
- **Achieves system privileges.** As opposed to more common malwares such as bankers, ransomwares and PoS scrapers, this APT hooked into the Operating System (OS) in order to appear as a legitimate OS process and to access system-wide settings.
- **Can be controlled without requiring Internet-connectivity.** Moker does not need an external communication point (such as a Command and Control – C&C server) to operate. It can also receive its commands locally, through a hidden control panel.

This means that a threat actor can also login say, via VPN using legitimate user credentials, and operate the malware on the infected device.

- **Takes great measures in order to bypass posthumous research once detected.** For example, Moker applied sophisticated anti-debugging techniques to avoid malware dissection and deceive researchers.

What are Moker's capabilities?

Moker targets Windows machines and:

- Takes complete control of the victim's machine by creating a new user account and opening a RDP channel to gain remote control of the victim's device
- Tampers with sensitive system files and modify system-security settings
- Takes screenshots, records web traffic, monitors key strokes and exiltrates files
- Injects itself into different system processes in order to replace legitimate code with malicious code during run-time

We're continuing to investigate this malware in our labs and will update accordingly.

Who's Behind Moker?

A test in our labs revealed that under certain circumstances Moker communicated with a server registered in Montenegro. The Montengro-based server was referred by several other domains registered in African countries. It's important to note however that these registered domains cannot give an indication of the threat actor's identity or physical location as it certainly makes sense to think that the threat actor either used compromised servers or purchased dedicated-only servers in other locations to confuse researchers and law enforcement agencies.

Interestingly, Moker did not necessarily need to be controlled from remote. A feature of the RAT includes a control panel that enables the attacker to control the malware locally. Consider a Local Access Trojan (LAT). We think this feature was added either for a threat actor to mimic a legitimate user (say, VPN'ing into the enterprise and then commanding Moker locally), or was inserted by the malware's author for testing purposes yet remained also in the production version.

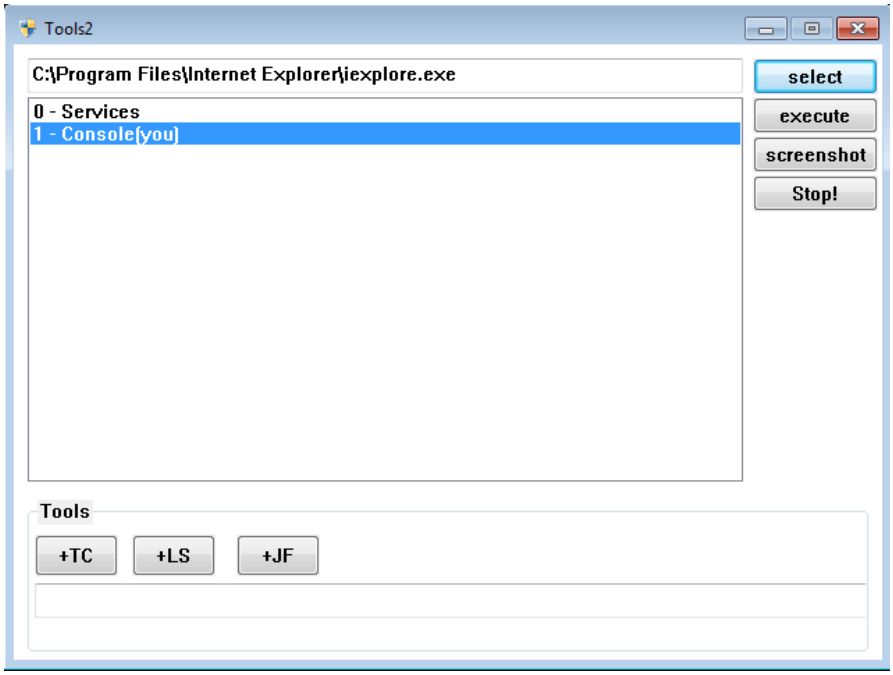

Figure 1: Remote vs Local Commanding of the Infected Machine

Moker's sophistication wasn't only in terms of its capabilities, but also in the measures it took to defend itself, including after it was caught. Its detection-evasion measures included encrypting itself and a 2-step installation (see below). Measures to protect itself from posthumous dissection included evading debugging techniques that are used by researchers, the addition of complex code and purposefully adding instructions to lead researchers in the wrong direction.

Obviously, this is a threat actor that invested a lot of resources in order to keep this malware stealthy.

How did the victim become infected?

Specifically for this campaign, we do not yet know how the malware infected the victim. The bottom line, however, is that this malware infiltrated the organization.

In general, malware can infect a machine in a variety of ways, such as sending a sophisticated phishing email, enticing the victim to click on a link or even plugging in a thumb drive.

How does Moker install itself?

Installation occurs in two stages. The two-stage installation is performed to defeat security measures such as sandboxing that rely on time-sensitive techniques:

1. **Planting a Dropper.** Moker first plants its "infrastructure", preparing the groundwork for full installation at a later stage. The Dropper itself does not appear malicious as it doesn't actually do any harm and so defeats the sandbox measures. Once planted in the machine, it can then easily receive the malicious payload at call of duty.
2. **Installing the Payload.** Once the Dropper is in place, it installs its second component – the malicious payload. The payload is either downloaded via an Internet connection, or loaded locally. It comes encrypted to defeat security measures that monitor the network and file systems. Once the it arrives in the victim's machine, the Dropper decrypts the payload and injects it into system processes.

How does Moker defeat security solutions and Windows' measures?

The APT performs the following in order to defeat detection:

1. **Code Packing.** This enables the malware to evade signature-based solutions such as Anti-Virus (AV) and network monitoring solutions that inspect traffic packets.
2. **Two-step installation.** This allows it to evade security solutions such as sandboxing and virtual machines (as stated in the above question "How does Moker install itself?")
3. **Vulnerability Exploitation.** In order to achieve system privileges both the Dropper and the payload had to bypass Windows' User Access Control (UAC). They did this by exploiting a known Windows design flaw. It's important to mention that this flaw is not a vulnerability in the sense of a buggy code, but rather a Windows' feature that is abused by threat actors.

Can we predict this malware to appear more in the wild?

This case might have been a dedicated attack. However, we do see that malware authors adopt techniques used by other authors. We won't be surprised if we see future APTs using similar measures that were used by Moker (such as bypassing security mechanisms and dissection techniques).

How can an organization protect itself against Moker?

As shown, well-established security measures and Windows' security mechanisms cannot stop the infiltration of Moker.

What we recommend is to recognize that infection is inevitable, and so to secure all data under the assumption that the environment is infected. Measures for securing the data include:

- Blocking in real-time all malicious outbound communications
- Preventing in real-time the malicious tampering of files
- Following up on actual malicious communicating/tampering attempts in order to perform attack forensics

A technical analysis of Moker appears on BreakingMalware - http://breakingmalware.com/uncategorized/moker-part-1-dissecting-a-new-apt-under-the-microscope

Get Technical!
Check out our researchers' blog - breakingmalware.com

POST TAGS RESEARCH

Subscribe to enSilo's Blog and Stay on Top of the

Latest Security Research and Industry News

Email*

SUBSCRIBE

Recent Posts

- Moker: A new APT discovered within a sensitive network
- Cyber-Security in 120 Secs: PoS Breaches, Ransomware Arrest and More
- Cyber-Security in 120 Secs: Fake Certificates, Privacy vs Security, and More
- AVG: the Clash of Security vs Privacy
- Cyber-Security in 120 Secs: Ransomware, CVS and More
- The Top 10 BlackHat 2015 Talks for the Security Researcher
- MS Patch Tuesday: A Look into 4 Vulnerabilities in the Windows Kernel
- Our Series A Funding: What it Means for Our Customers and Prospects
- MS June Patch Tuesday: Double Trouble in the Microsoft Kernel..
- The 10 RSA Talks to Get the Most Out of the Conference

Posts by Topic

- Research (7)
- Industry (3)
- Weekly Security News (3)
- Business (2)
- Windows (2)

Archive by Month

- September 2015 (3)
- March 2015 (2)
- April 2015 (2)
- June 2015 (2)
- October 2015 (2)
- February 2015 (1)
- July 2015 (1)
- August 2015 (1)