Rig Exploit Kit Drops Predator The Thief InfoStealer and CrySIS Ransomware

Author: James Barnett

Overview

On 17 November, Broad Analysis reported[1] a campaign that used Rig exploit kit to distribute an infostealer known as Predator The Thief, followed by a variant of CrySIS ransomware.

Customer Impact

Rig is an exploit kit (EK) used to attack vulnerabilities in systems in order to distribute malware or perform other malicious activities. Rig was first discovered in 2014, and its continued popularity amongst threat actors is a testament to its efficacy.

Predator The Thief is an infostealer used to harvest login credentials, cryptocurrency wallets, and other types of sensitive information from targeted systems.

CrySIS is a ransomware that extorts victims by encrypting files on their system and demanding a fee to decrypt them.

Campaign Analysis

The campaign reported by Broad Analysis used malicious advertisements (malvertisements) placed on legitimate websites to redirect vulnerable users to malicious websites containing Rig exploit kit, which was in turn used to deliver Predator The Thief and a CrySIS variant.

The original report referred to this variant as “Bot ransomware” due to the file extension it uses; our report will refer to it as CrySIS because it shares the same behaviors and CrySIS has a long history of releasing new versions with different file extensions.[2]

Attack Chain

The attack chain begins when the victim encounters one of Rig's malvertisements on an otherwise legitimate website. This malvertisement contains an inline frame (IFrame) that redirects the victim to a malicious website controlled by the Rig operator.

This website contains a "gate" page that profiles the victim's system to identify potential vulnerabilities. When the gate identifies that a victim's system is vulnerable it redirects them to a landing page that contains Rig EK, which exploits the previously identified vulnerabilities to infect the victim's system with one or more malicious payloads.

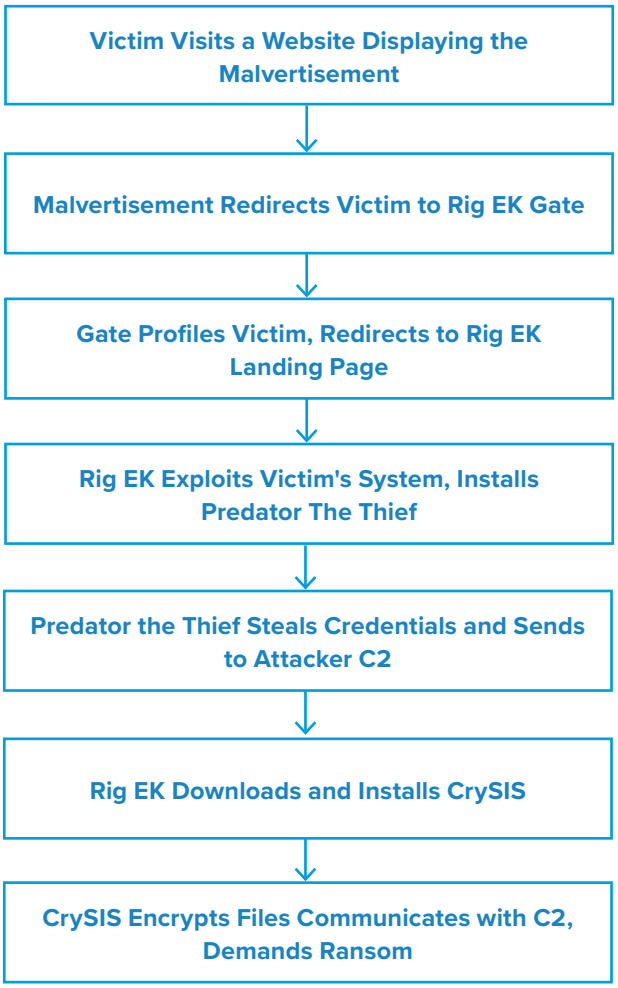
The first malicious payload that Rig EK deployed in this campaign was Predator The Thief. Upon execution, Predator The Thief unpacks its obfuscated configuration data and loads it into memory.[3] This configuration data includes the domain name of its command and control (C2) along with various system paths and filenames that it uses to steal credentials.

Once the configuration is loaded the malware proceeds to steal cryptocurrency wallet information along with saved credentials from web browsers, FTP clients, chat applications, and various other targets. It also uses the Windows GetFileAttributesA function to scan the user's Desktop, Documents, and Downloads folders and steals any files with the following extensions: ".doc", ".docx", ".log", ".txt".

Once Predator The Thief is done stealing credentials it generates a log file that contains information about the victim's system (e.g. hardware, OS version, user accounts, etc.), along with performance metrics for the malware itself. It then creates an archive containing all the stolen data and log files, then sends this archive to its C2 with an HTTP POST request.

The second payload that Rig EK deployed in this campaign was CrySIS ransomware. When CrySIS executes, it creates registry entries to maintain persistence and uses the Windows Volume Shadow Copy Service (VSS) to delete the victim's existing hard drive backups.[4]

It then proceeds to encrypt nearly every file on the victim's system aside from critical system files and files used by the malware itself. During the encryption process CrySIS will send copies of some of the victim's files to its C2 based on their original file formats, presumably so that the attacker can scan them for credentials and other valuable information. When the encryption process is complete, CrySIS creates a ransom note on the desktop that directs the victim to send the attacker a certain number of Bitcoins to recover their files.



Vulnerabilities & Mitigation

Rig EK uses various known software exploits to compromise vulnerable systems and install a variety of malware payloads. Infoblox recommends the following methods for preventing and mitigating attacks related to Rig EK, Predator The Thief, and CrySIS.

- Keep computers and all endpoints up-to-date with the latest security patches to block known vulnerabilities that could be targeted by threat actors.
- Keep internet browsers updated; most modern browsers have default settings that enable automatic updates, but others may require more user interaction.
- Use ad blockers to help protect against malvertising, and strong antivirus software to detect and clean unwanted browser programs.
- Back up data and systems regularly to minimize the potential impact of ransomware in general.
- Ideally, store backup data off the network.

Endnotes

1. https://broadanalysis.com/2019/11/17/rig-exploit-kit-delivers-predator-the-thief-and-bot-ransomware/
2. https://www.cyber.nj.gov/threat-profiles/ransomware-variants/crysis-dharma
3. https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/
4. https://blog.malwarebytes.com/threat-analysis/2019/05/threat-spotlight-crysis-aka-dharma-ransomware-causing-a-crisis-for-businesses/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com