GoldenEye-Petya security note

Threat Intelligence Labs

June 2017

A new ransomware campaign, like the WannaCry incident of May 12th, is impacting a number of companies globally. The ransomware in this case is a variant of the GoldenEye-Petya family that has been modified to spread directly through the network using the same exploit as WannaCry. The ongoing malware attacks mainly target Windows-based corporate devices. To date, Nokia has not observed a significant increase in this exploit in networks protected by NetGuard Endpoint Security (NES). Nokia will continue to monitor the situation and update customers as appropriate.
1  What is GoldenEye?

GoldenEye is a ransomware. Ukraine's government, National Bank and biggest power companies are reported to have been attacked as have airlines and metro services in the c. There have also been reports that Maersk, Merck, DLA Piper, WPP and the Russian oil company Rosnoft have been attacked.

2  What does it do?

The infection impacts Windows-based servers, desktops and laptops. Once a device is compromised, the files are encrypted and a US$300 ransom is demanded for the decryption keys. The malware also encrypts key components of the device's file system and then shuts it down, rendering it unbootable until the ransom is paid.
3 How does infection occur?

Petya spreads through malicious Office attachments and email. This gets through the front door and onto any target system that can be exploited via social engineering. Once the malware is installed, it looks for other systems to exploit using EternalBlue. This is the same vulnerability used by WannaCry to exploit any system via lateral movement. Encryption is at a low level using the Master File Tree tables for NTFS and overwrites the Master Boot Record (MBR) with a ransomware warning. Therefore a reboot must be done instantly or the MBR can be compromised.

How does it work?

GoldenEye has two layers of encryption, locking up both files and the computer's file system. The malware forces an infected PC to reboot as soon as it finishes encrypting files, so ransom demands will be visible immediately. Reports indicate that there is also a hidden Trojan on Petya that steals victims' usernames and passwords. The difference between Petya and WannaCry is that Petya apparently does not have a kill-switch domain that could be accidentally triggered. GoldenEye ransomware used EternalBlue, the NSA exploit that fueled WannaCry's spread.

EternalBlue (MS17-010) is a Windows SMB vulnerability. A patch for this vulnerability was released by Microsoft in mid-March, after a leaked NSA rootkit called DoublePulsar, which used the vulnerability, became publicly available.

4 What has Nokia done?

A signature SID:2024216/Win32.Backdoor.DOUBLEPULSAR is already deployed to NES customers that detects the SMB-based infection attempts using the EternalBlue vulnerability. The IP addresses in the raw events identify which subscribers are infected and could be used by service providers to block infected devices: this could help prevent spread of the malware. The rule that detects this SMB infection associated with the ransomware has been deployed since May 1st.

Nokia Threat Intelligence Labs is analyzing a copy of the ransomware, GoldenEye/Petya. We will provide updates on the availability of new related signatures.
5 Recommendations

The ransomware spreads rapidly through corporate networks using the same exploit as Wannacry, so the remediation steps that were put in place for that incident will be effective against this latest outbreak.

Some key recommendations include:

- Stay up to date with patching. Microsoft’s Security Response Center (MSRC) Team addressed the vulnerability via MS17-010 released March, 2017. Audit systems to ensure latest patches are applied.
- Where possible block port 445 at the network perimeter and between any major network segments. This will prevent the ransomware from spreading directly from computer to computer through the network using the EternalBlue vulnerability.
- Proactively audit the security configuration policies of network and perimeter firewalls.
- Ensure privileged access controls are in place for critical Operational Technology (OT) systems - that is, the workstations used to operate and manage critical infrastructure and other key assets. Rotate administrative credentials on all OT systems.
- If a system is compromised, immediately disconnect it from the network to prevent further damage.
- To recover an infected system, reformat the disks, reinstall the operating system and restore the files from the last good backup.