Targeted Email Attacks- Locky

A Detailed Analysis from FortiGuard Labs

In October of 2015, the Cyber Threat Alliance—a multi-vendor security consortium—issued a detailed report on CryptoWall ransomware that encompassed more than 4000 malware samples and 800 command and control servers. Since that time the prevalence and profile of ransomware has continued to escalate, including the introduction of new families such as Locky, which we profile here.

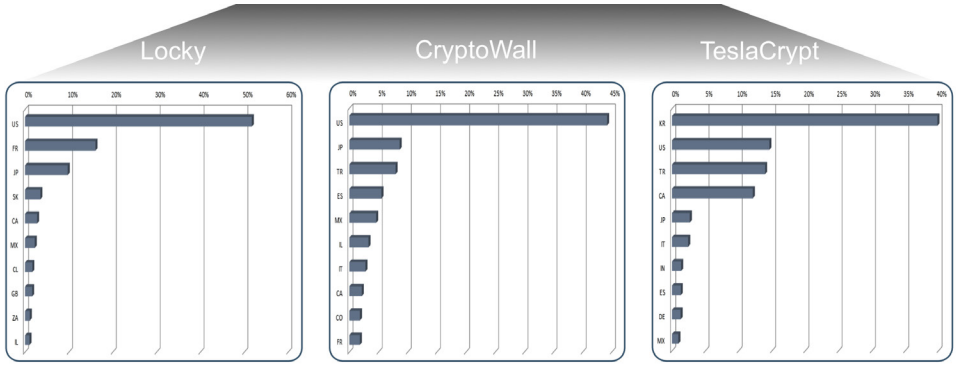

FIGURE 1: TOP 3 RANSOMWARE FAMILIES 2Q16

In this threat brief, we will examine what is changing in the world of ransomware and present concrete recommendations to reduce the risk of an incident.

DEFENSE AGAINST RANSOMWARE

Although the ransom demanded to decrypt files is often a modest amount (thousands of dollars) among operational expenses there are far better ways to address the risk ransomware.

So, what do we recommend? Preparation, Prevention and Process.

Lifecycle of Advanced Ransomware

Step 1: Reconnaissance and Incursion

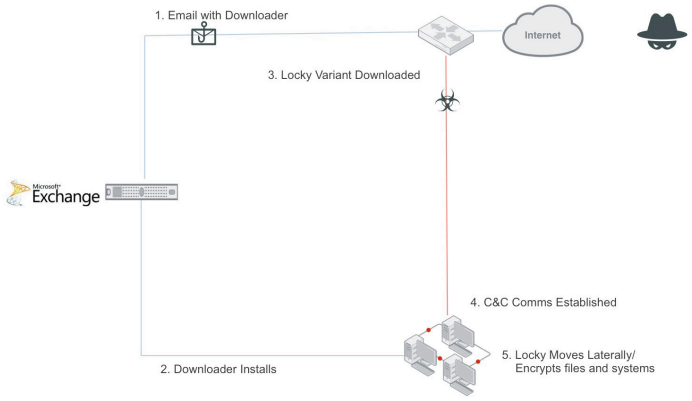

FIGURE 2: A COMMON LOCKY ATTACK LIFECYCLE

Sophisticated cybercriminals typically start with reconnaissance on the target organizations. Given that the most common delivery vehicle for Locky at the time of this writing is via email phishing, this includes acquisition or creation of an email address list.

While Locky can target personal email addresses, it is often easier/more likely for cyber criminals to guess corporate email addresses since employee names are often available and there are a limited number of email address conventions commonly used (like firstname.lastname@company.com) Further, what's typically sent is an innocuous appearing Word document with malicious macros embedded that facilitate the installation of malware on the user's computer.

While nearly all enterprises have email security in place, many put it in place years ago and find that it can't handle the latest threats like ransomware. Ensuring that your email security solution has kept pace with the changing threat landscape, continues to demonstrate high effectiveness, and includes integrated sandboxing is critical to stopping Locky and related attacks.

Step 2: Attempt to Exploit and Enter

As mentioned, the initial attack code itself is generally hidden within a Word document and utilizes support for macros in order to install on the end user system. These are typically small snippets of initial code that establish connections to external attacker-controlled sites to download subsequent malware components.

Because of their simplicity, these snippets are simple to change to avoid detection. At the time of writing, JS/Nemucod (a javascript downloader) was one of many methods used by attackers to download ransomware. In just two days, one variant sought entry at ~15,000 locations (and was blocked) more than 4 million times.

Complementing email security measures with strong network security elements, especially those that can also feed into and receive intelligence out of a shared sandbox is critical for a holistic approach to tackle layered defense against ransomware like Locky.

Step 3: Establish Communications

Locky initially used a domain generation algorithm (DGA), in conjunction with the RTDSC function to get a counter that determined the domain used, to contact the command and control (C&C) server. This helps the cybercriminal rotate in new domains and minimize the chance of reputation-based blocking by network security controls.

Further, it encrypts the communication with the outside C&C in an attempt to avoid detection. Various encryption methods have been used in just these first few months of its existence: first hard-coded RSA key encryption, then hard-coded custom encryption algorithms and most recently RSA encryption based on Windows APIs.

```
v7 = 0;
hHash = 0xCD43EF19u;
if ( *(_DWORD *)(lpOptional + 16) )
{
  do
  {
    v8 = *(_DWORD *)(lpOptional + 20);
    if ( v8 < 0x10 )
      v9 = lpOptional;
    else
      v9 = *(_DWORD *)lpOptional;
    v10 = *(_BYTE *)(v9 + v7);
    if ( v8 < 0x10 )
      v11 = lpOptional;
    else
      v11 = *(_DWORD *)lpOptional;
    v12 = __ROR__(hHash, 5);
    v13 = __ROL__(v7, 13);
    *(_BYTE *)(v11 + v7) = v10 ^ (v12 - (_BYTE)v13);
    v14 = __ROL__(v10, v7 & 0x1F);
    v15 = __ROR__(hHash, 1);
    v16 = v15 + v14;
    v17 = __ROR__(v7++, 23);
    hHash = (v17 + 0x53702F68) ^ v16;
  }
  while ( v7 < *(_DWORD *)(lpOptional + 16) );
}
```

FIGURE 3: ENCRYPTED COMMUNICATIONS

Step 4: Malware Installation

Because the communications between the compromised system and the C&C server are encrypted, delivery of components is often hidden from network and web security solutions if SSL inspection is not enabled. And since the code is hosted and delivered from outside the organization it can be easily rotated by the cybercriminal to stay ahead of reactive signature updates.

In addition, more recent versions of Locky use various evasion techniques to avoid more dynamic analysis like sandboxing. At the time of writing, sophisticated sleeps, in which an internal rather than system clock is used to calculate time and even the random determination of how long to sleep, are common. It is essential that your sandbox solution include strong anti-evasion techniques: not just accelerating the system clock to simulate the passage of time but ideally using emulation (reading rather than running the code) to look for VM-evasion instructions.

Step 5: Encryption and Ransom

Once the ransomware payload is installed and runs, it will immediately encrypt files on the system including (at the moment) fixed, removable, and RAM disk drives. Thereafter the ransom message is presented, demanding payment in bitcoins for the key to decrypt these drives.

Security Recommendations

Although the ransom demanded to decrypt files is often a modest amount (thousands of dollars) among operational expenses there are far better ways to prepare for ransomware and they are important because:

- Paying the ransom does not guarantee you will get a decryption key
- The more money cybercriminals make with ransomware today, the more common ransomware will become tomorrow
- We don't know what else cybercriminals might do once inside the network while you are busy dealing with ransomware
- Being held hostage doesn't reflect well on the security and IT department
- The recommended practices don't have to be hard or expensive.
- So, what do we recommend? Preparation, Prevention, and Process.

Preparation

Preparation should include, first and foremost, a backup and solution for end user systems. Hopefully you already have disaster recovery systems and plans in place for critical infrastructure but the ability to restore end-user systems is a different matter and one often overlooked. Given that PC backups will help in the event of lost, stolen, or broken computers, as well as ransomware this seems a no-brainer.

Prevention

But no need to concede defeat to a ransomware attack without trying to stop them. Prevention can happen at multiple levels. First, ensure a strong email security solution is in place, as this is the common vector of attack at the moment. Second, extend email security with advanced inspection, such as sandboxing, as this provides the opportunity to hold messages for advanced analysis and block even those that contain brand new malware. We mention sandboxing because the act of encrypting files is a readily visible and clearly malicious indicator when it occurs.

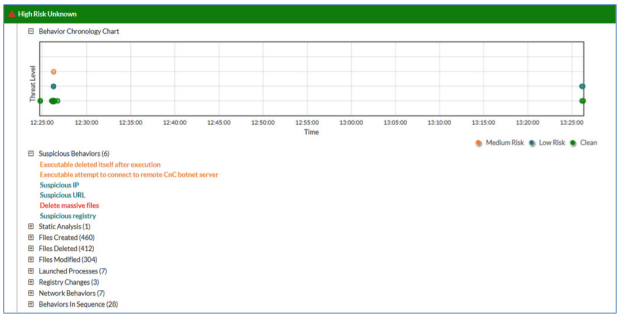

FIGURE 4: SANDBOX BEHAVIOR SUMMARY

Second, if you are looking for broader preventive coverage, make sure that you can hook your endpoint protection into your sandbox solution. This integration can cover all vectors of delivery and share intelligence about new ransomware variants from the sandbox to every device on-and off-premises to immediately raise protections and/or remove files after the first new piece of ransomware is received.

Third, if tying in to your endpoint solution is not possible, at least ensure your sandbox can feed that same intelligence to your firewall to quarantine devices, block command and control traffic, and prevent delivery of new ransomware variants after detection.

Process

Should one or more of those preventative steps not be possible at the outset, at least establish a process to manually get information from a sandbox out to the endpoints and firewalls.

Key intelligence, or indicators of compromise (IoC) that you should start with include:

- Hash or signatures for files deemed to be malicious or high risk after sandbox analysis
- IP addresses for the source of the initial delivery, subsequent communications, and downloads
- Names of processes and registry settings changed in the course of the attack
- Users and/or devices for whom the attack was intended

All of this intelligence can be used to respond to the attack, contain its impact, mitigate the ultimate impact, prevent similar intrusions, and aid in user awareness and training.

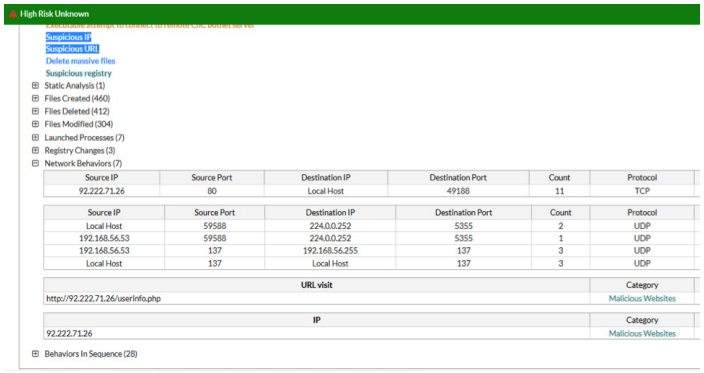

FIGURE 5: EXAMPLE IoCs

Conclusion

While ransomware attack techniques vary, FortiGuard researchers often see the following evasion techniques used to bypass traditional security technologies:

- Emails sent from compromised systems with a mixed reputation based on legitimate email during the day and bot-controlled attacks at night
- Socially engineered messages, links, and attachments aimed at more security-conscious end users
- Encrypted, compressed, or password-protected attachments to evade static antimalware inspection
- Fresh command & control sites that last only days or even hours thanks to fast flux and other techniques
- Encrypted communications that bypass IPS and other forms of network behavior analysis

Make sure that your security defenses are adequate to overcome these and other attack techniques for the strongest defense against ransomware.

Advanced Threat Protection

The most common technology considered for advanced threat protection in response to the evasion techniques above is sandboxing, which provides the dynamic analysis necessary to uncover today's targeted attacks, as well as the threat intelligence to thwart them. Further, sandboxing is increasingly available as an integrated component of existing infrastructure rather than a stand-alone solution operating independently. An integrated solution can speed up and automate prevention and mitigation.

In this case, Fortinet's FortiMail Secure Email Gateway and FortiSandbox provide an integrated approach to preventing the delivery of previously unknown ransomware via email the very first time it seeks entry and before delivery to the end user. To extend similar protections to identify and respond fast to ransomware delivered as web downloads, consider adding FortiGate Next Generation Firewalls to the solution. And to protect users on and off network, as well as contain ransomware that may have slipped through via other vectors, add in FortiClient Endpoint Protection for the broadest coverage.

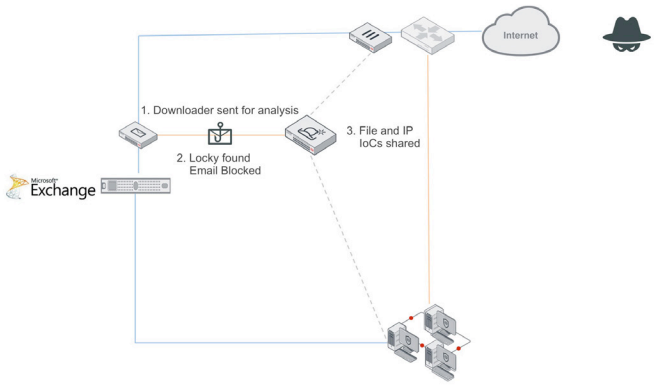

FIGURE 6: ATP SOLUTION INTEGRATION

For more information on the FortiMail-FortiSandbox integration, read "Playing Safely in the Sandbox" http://www.fortinet.com/resource_center/whitepapers/fortimail-playing-safely-sandbox.html

Of course, adding the dynamic analysis of a sandbox is just one way to address the security risk posed by advanced threats. Fortinet recommends organizations consider a more cohesive approach designed to seamlessly align prevention, detection, and mitigation of attacks for a continuous cycle of improvement. This approach is outlined in the Fortinet Advanced Threat Protection framework.

For more on this framework please visit http://www.fortinet.com/solutions/advanced-threat-protection.html.

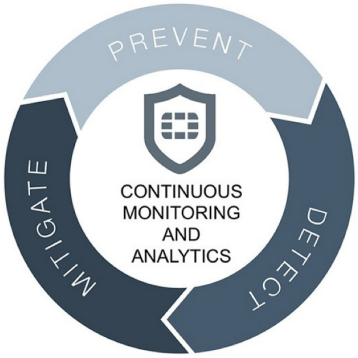

FIGURE 7: FORTINET'S ADVANCED THREAT PROTECTION FRAMEWORK

Many thanks to the FortiGuard team. For more information on Locky, please visit the following articles on our security research blog. https://blog.fortinet.com/tag/ransomware-1

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

June 10, 2016