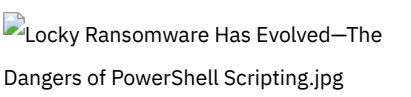
# Locky Ransomware Has Evolved—The Dangers of PowerShell Scripting

December 14, 2016
by SentinelOne




It's no secret that ransomware is taking the cybersecurity community by storm. In fact, a recent survey discovered that 48% of organizations have experienced a ransomware attack in the last 12 months.

One of the biggest challenges companies have when defending against ransomware is the same challenge when defending against zero-day threats—cyber attackers have proven time and time again that they can stay one step ahead of signature-based solutions.

The creators behind the Locky ransomware family are no exception. In the last few months, the Locky ransomware family has evolved, leveraging PowerShell scripting to stay ahead of cyber defenses—and you have to be ready.

## Locky Ransomware—The Shift from WSF Files to LNK Files and PowerShell Scripting

The most popular way that Locky ransomware has been distributed has been through malicious ZIP files and email spam campaigns. Recent iterations have used these ZIP files to distribute malicious WSF files, but the cybersecurity community has caught on.

As cybersecurity professionals block these malicious WSF files and mitigate the use of Nemucod for Locky to test for sandbox environments, Locky creators have turned to new means of infection.

The Microsoft Malware Protection Center recently identified a trend away from WSF files in favor of LNK files and PowerShell scripting. These LNK shortcut files install Locky ransomware by automating infection operations rather than relying on traditional user downloads of WSF files—all of which is made possible by the universal PowerShell Windows application.

But what is PowerShell scripting and why is it causing so many cybersecurity problems?

## A Closer Look at PowerShell Scripting and Cybersecurity Implications

Unfortunately, cyber criminals have been able to leverage PowerShell for their attacks for years. In a recent report, the application was found to be involved in nearly 40% of endpoint security incidents. While attackers have been finding weaknesses in the Windows operating system for years, it's clear that there's something problematic with PowerShell scripting.

One issue is that so many system admins aren't as familiar with PowerShell scripting as attackers. It's important to really understand what PowerShell is used for in the enterprise. Here's what Microsoft has to say about the application:

*"Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Built on the .NET framework, Windows PowerShell helps IT professionals and power users control and automate the administration of the Windows operating system and applications that run on Windows."*

While the scripting language can be a powerful tool for system administration, Locky creators are using its automation capabilities to their advantage. With 97% of malicious spam campaigns being attributed to Locky ransomware, it's clear that we need to get ahead out ahead of the family's creators.

## Get Proactive When It Comes to Ransomware and Exploit Scripting

We can't grow complacent with the new ransomware reality we find ourselves in. Simply paying the ransom doesn't always unlock your files, meaning your systems can be disrupted and (if you aren't prepared) there's nothing you can do about the ensuing data loss.

As ransomware families and malware in general continues to evolve, you can't rely on reactive cybersecurity solutions to protect your network and data. With Locky adopting PowerShell scripting, it's clear that attackers are getting better at avoiding detection and your organization has to keep up.

If you want to learn more about the problem with reactive ransomware solutions and how you can become more proactive in your defenses, download this free white paper, *Ransomware Is Here: What Can You Do About It?*.

---

**Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.**

### Read more about Cyber Security

- Mobile Malware — The Market for Mobile Exploits Is Heating Up
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
- Lazarus 'Operation In(ter)ception' Targets macOS Users Dreaming of Jobs in Crypto
- From the Front Lines | 8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts
- BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar