Cybercriminals Increasingly Trying to Ensnare the Big Financial Fish

secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Counter Threat Unit Research Team

Threat groups such as GOLD KINGSWOOD are using their extensive resources and network insights to target high-value financial organizations around the world. Thursday, September 27, 2018 *By: Counter Threat Unit Research Team*

When the security industry characterizes the e-crime threat landscape, there is a temptation to focus on the everyday scams and high-volume aspect of the criminal threat landscape. These criminals are not particular about targets if there are financial rewards at the end. Obvious examples of these types of scams are the widely distributed malware aimed at stealing bank account credentials and the ransomware disseminated through large-scale spam phishing campaigns.

These criminals can earn a decent income over time netting smaller "financial fish" through opportunistic scams. However, some cybercriminals are setting their aims higher and focusing on much larger fish. Secureworks® Counter Threat Unit™ (CTU) researchers have observed a growing threat from sophisticated threat actors who pursue high-value targets such as banks and financial services companies and have the capability to exploit and monetize access to payment and other financial systems. CTU™ researchers call one of these threat groups GOLD KINGSWOOD.

GOLD KINGSWOOD: An advanced persistent cybercrime group

GOLD KINGSWOOD (also known as the Cobalt Gang) is a capable, sophisticated, and financially motivated criminal threat group that has successfully compromised financial organizations since at least 2016. The group uses targeted network intrusion tactics to locate, access, and abuse systems that can be monetized. As of March 2018, the threat actors had reportedly stolen approximately $1.2 billion USD through their global operations. Unlike most criminally motivated e-crime actors observed by CTU researchers, GOLD KINGSWOOD's tactics, techniques, and procedures (TTPs) are similar to attributes of traditional government-sponsored or espionage-driven threat actors. For example, in operations against the First Commercial Bank (FCB) of Taiwan, GOLD KINGSWOOD used custom malware that leveraged CSCWCNG.dll, which is specific to the ATM hardware used at FCB. After receiving confirmation of the ATM locations where money mules were waiting, the threat actors executed commands to dispense money from the machines. This incident demonstrated GOLD KINGSWOOD's vast technical and human resources.

GOLD KINGSWOOD serves up a SpicyOmelette

In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities. GOLD KINGSWOOD delivered SpicyOmelette through a phishing email containing a shortened link that appeared to be a PDF document attachment. When clicked, the link used the Google AppEngine to redirect the system to a GOLD KINGSWOOD-controlled Amazon Web Services (AWS) URL that installed a signed JavaScript file, which was SpicyOmelette.

CTU analysis of one of GOLD KINGSWOOD's campaign using SpicyOmelette (DOC2018.js) exposed additional sophisticated methods to compromise targets. A valid digital certificate was used to sign the malicious script. Windows Scripting Host supports the inclusion of digital signatures, and Figure 2 shows how the signature was appended to the script. Depending on the security profile of the victim's system, a pop-up notification may have warned about running external content. However, the system would have also indicated that the script was signed by a valid and trusted certificate authority (CA). SpicyOmelette also passed parameters to a valid Microsoft utility, which allowed the threat actors to execute arbitrary JavaScript code on a compromised system and bypass many application-whitelisting defenses.

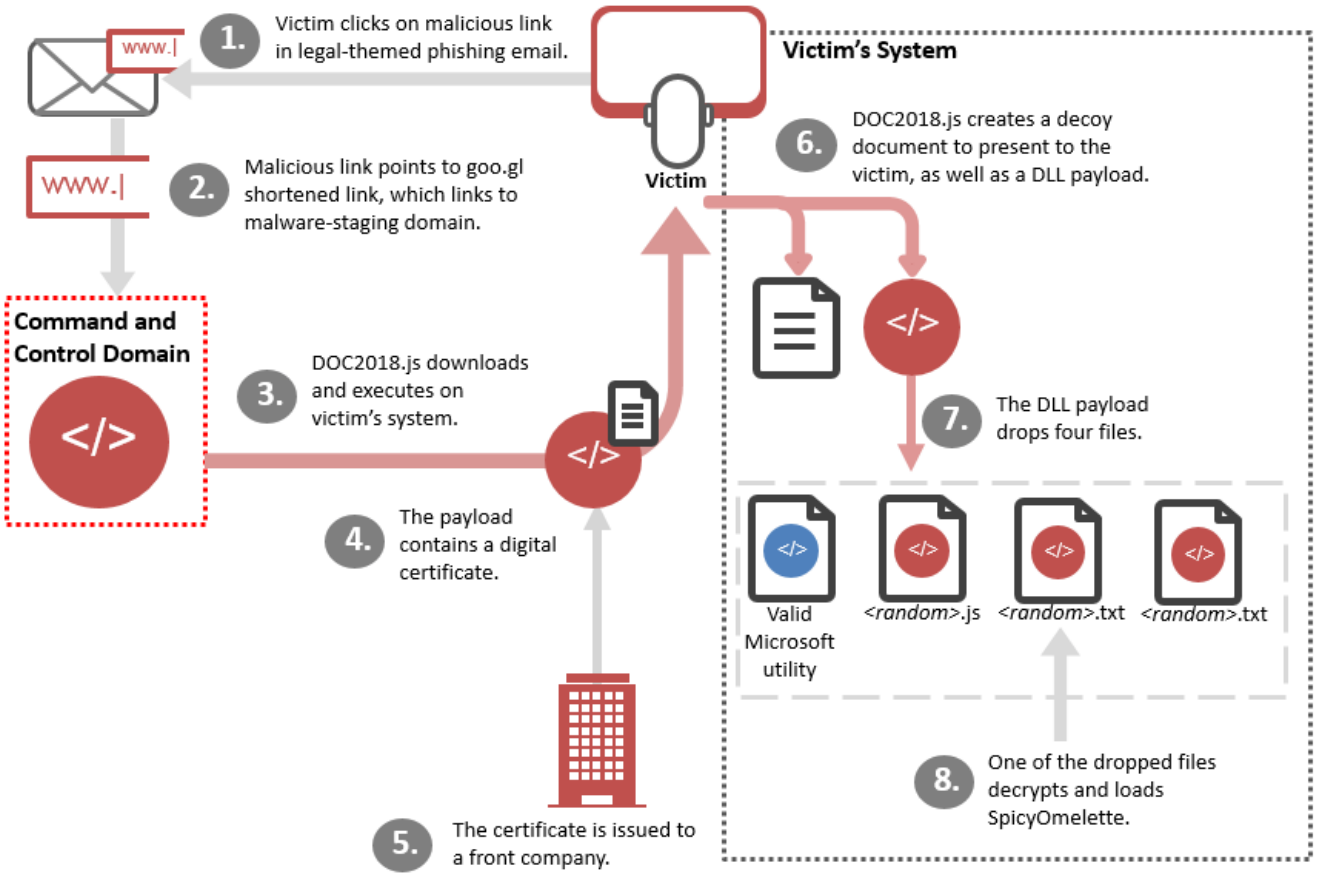

Figure 1. SpicyOmelette infection chain. (Source: Secureworks)

Once installed, SpicyOmelette provides an ideal foothold onto a targeted system for GOLD KINGSWOOD. It enables the threat actors to perform various actions:

- profile the infected system for information (e.g., running software, system name, IP address)
- install additional malware onto the system
- check for the presence of 29 different antivirus tools

The access provided by SpicyOmelette and other post-compromise tools regularly used by GOLD KINGSWOOD helps the threat actors escalate privileges on a system by stealing account credentials, survey and evaluate the compromised environment, identify desirable systems (e.g., payment systems, payment gateways, ATM systems), and deploy malware specifically designed to target those systems.

Conclusion

The ‘advanced' nature of GOLD KINGSWOOD intrusions stems from the care and focus that the threat actors exhibit, specifically finding and accessing systems of interest. Arrests of suspected GOLD KINGSWOOD operators in March 2018 did not deter the threat group's campaigns, likely due to its vast network of resources. CTU researchers expect GOLD KINGSWOOD's operations and toolset to continue to evolve, and financial organizations of all sizes and geographies could be exposed to threats from this group. The threat group's detailed understanding of financial systems and history of successful campaigns make it a formidable threat.