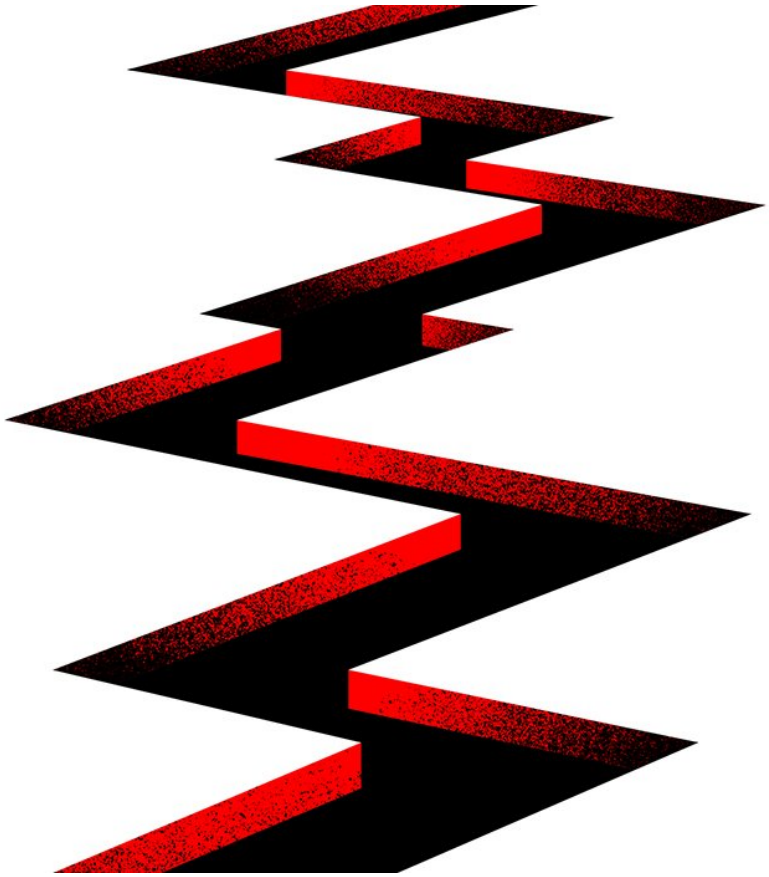
Falcon OverWatch Detects Novel IceApple Framework

crowdstrike.com/blog/falcon-overwatch-detects-iceapple-framework/

Adrian Justice May 11, 2022



The CrowdStrike Falcon OverWatch™ proactive threat hunting team has uncovered a sophisticated .NET-based post-exploitation framework, dubbed IceApple. Since OverWatch's first detection in late 2021, the framework has been observed in multiple victim environments in geographically distinct locations, with intrusions spanning the technology, academic and government sectors.

The emergence of new and evolving IceApple modules over the past year indicates that this framework remains under active development.

To date, IceApple has been observed being deployed on Microsoft Exchange server instances, however it is capable of running under any Internet Information Services (IIS) web application. As such, ensuring all web applications are fully patched is critical to ensuring IceApple doesn't end up in your environment.

For a detailed look at IceApple download OverWatch's research paper that explores in depth how IceApple was found, the functionality of all currently discovered modules, and how these modules interact.

IceApple Likely Intended for Long Running Campaigns

IceApple is a post-exploitation framework — this means it does not provide access, rather it is used to further mission objectives after access has already been achieved. OverWatch's investigations have identified 18 distinct modules with functionality that includes discovery, credential harvesting, file and directory deletion and data exfiltration. OverWatch has observed evidence of adversaries repeatedly returning to victim environments to carry out their post-exploitation activities.

IceApple uses an in-memory-only framework that highlights the adversary's priority of maintaining a low forensic footprint on the infected host. This is typical of long-running objectives aimed at intelligence collection and aligns with a targeted, state-sponsored mission. While the observed targeted intrusions align with China-nexus, state-sponsored collection requirements, at this time CrowdStrike Intelligence has not attributed IceApple to a named threat actor.

IceApple has a number of features to help it evade detection. Detailed analysis of the modules suggests that IceApple has been developed by an adversary with deep knowledge of the inner workings of IIS software. One of the modules was even found to be leveraging undocumented fields that are not intended to be used by third-party developers.

Efforts to blend into the victim environment are also seen with the assembly file names themselves. At first glance they appear to be expected IIS temporary files generated as part of the process of converting ASPX source files into .NET assemblies for IIS to load. Closer inspection is required to identify that the file names are not randomly generated as would be expected, and the way the assemblies are loaded falls outside of what is normal for Microsoft Exchange and IIS. OverWatch threat hunters' familiarity with how systems should operate, and also how adversaries attempt to corrupt these systems is what enabled hunters to quickly identify this suspicious activity.

How OverWatch Found IceApple

OverWatch regularly sees adversaries use .NET assemblies as a way to load additional functionality post-exploitation. Reflectively loading .NET assemblies, which involves executing the assembly directly within the memory of a process, can be a powerful and potentially stealthy way for adversaries to pursue their mission objectives. As such, OverWatch threat hunters have been actively developing detections for reflective .NET assembly loads.

In late 2021, one of Falcon OverWatch's in-development detections for reflective .NET assembly loads triggered on a Microsoft Exchange OWA server belonging to a customer who had recently started a trial of the Falcon platform. Eagle-eyed threat hunters identified anomalies in the assembly files and quickly reached out to the victim organization to notify

them. OverWatch then worked with the customer to configure the Falcon sensor to extract the contents of reflectively loaded .NET assemblies across the customer's endpoints giving OverWatch increased visibility and facilitating closer inspection of IceApple's functionality.

OverWatch Provides Agile Defense in the Face of Evolving Threats

IceApple is a highly sophisticated IIS post exploitation framework, however, it is by no means alone. OverWatch regularly identifies new reflectively loaded .NET assemblies of various levels of sophistication.

The CrowdStrike Falcon® platform detects all currently known IceApple module loads, while OverWatch actively hunts new IceApple modules. Threat hunting is a crucial piece of the defensive puzzle when it comes to novel and stealthy adversary tools like IceApple. CrowdStrike threat hunters draw on their extensive experience of what "normal" looks like in enterprise environments, knowledge of adversary behavior, and up-to-the-minute threat intelligence to preempt where the next threat might emerge. This feeds the development and testing of hypotheses that enhance the hunt and curtail adversary attempts to evade technology-based defenses. OverWatch's systematic workflows also ensure that the detailed analysis of IceApple will also feed back into continuous improvement and fine tuning of hunting leads.

The discovery of IceApple was the result of one such experimental hunting lead, and ultimately led to the discovery of attempted intrusions in multiple victim environments.

Additional Resources

- *Read the 2021 Threat Hunting Report blog or download the report now.*
- *Learn more about Falcon OverWatch's proactive managed threat hunting.*
- *Discover the power of tailored threat hunting OverWatch Elite provides customers in this blog post.*
- *Watch how Falcon OverWatch proactively hunts for threats in your environment.*
- *Read more about how part-time threat hunting is simply not enough in this blog post.*
- *Learn more about the CrowdStrike Falcon® platform.*