Thawing the permafrost of ICEDID Summary

elastic.co/security-labs/thawing-the-permafrost-of-icedid-summary

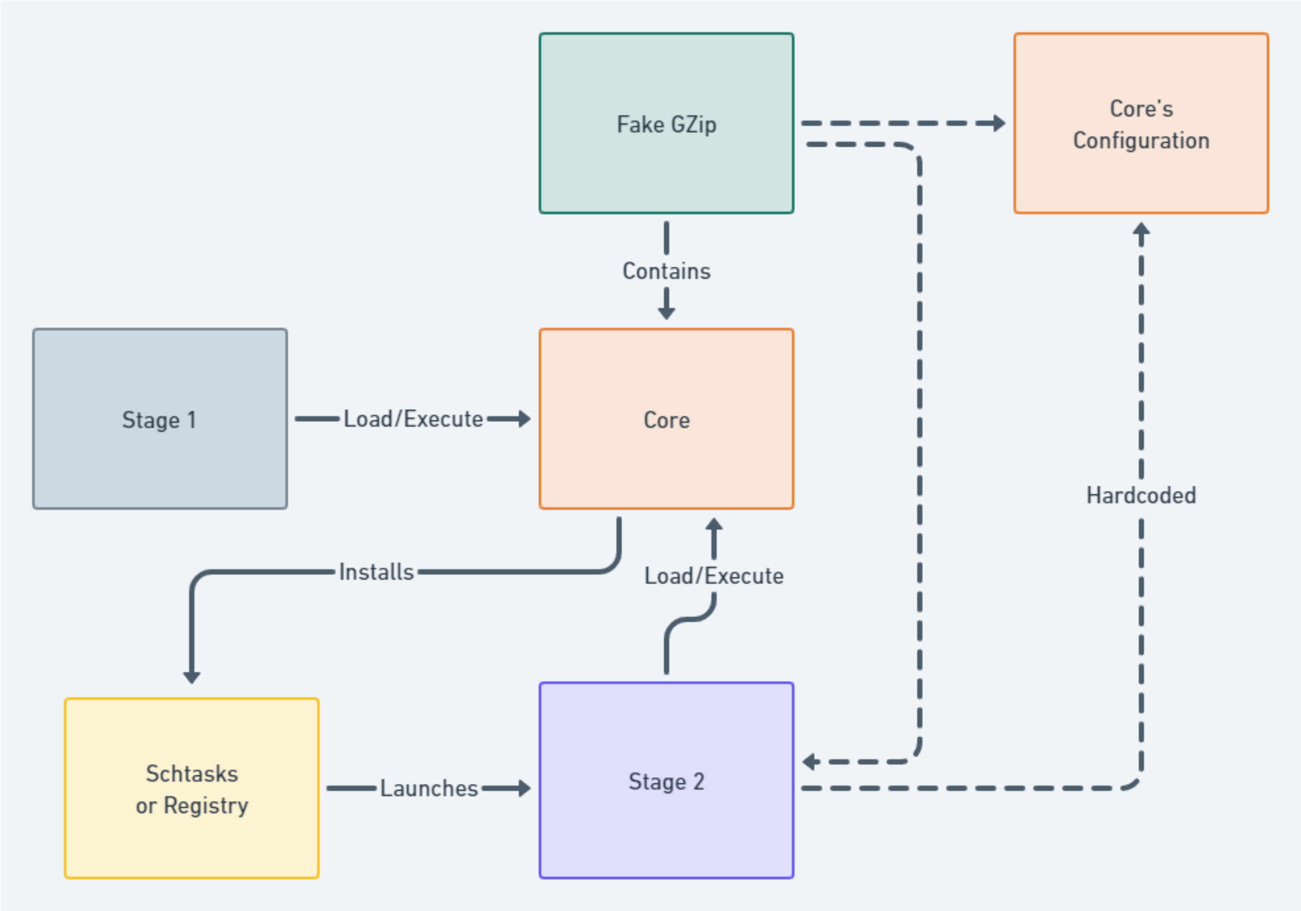
Elastic Security Labs details a recent ICEDID GZip variant

ICEDID is a malware family first described in 2017 by IBM X-force researchers and is associated with the theft of login credentials, banking information, and other personal information. ICEDID has always been a prevalent family, but has achieved even more growth since EMOTET's temporary disruption in early 2021. ICEDID has been linked to the distribution of other distinct malware families including DarkVNC and COBALT STRIKE. Regular industry reporting, including research publications like this one, help mitigate this threat.

Elastic Security Labs analyzed a recent ICEDID variant consisting of a loader and bot payload. By providing this research to the community end-to-end, we hope to raise awareness of the ICEDID execution chain, highlight its capabilities, and deliver insights about how it is designed.

Execution Chain

ICEDID employs multiple stages before establishing persistence via a scheduled task and may retrieve components from C2 dynamically. The following diagram illustrates major phases of the ICEDID execution chain.



Research Paper Overview

Elastic Security Labs described the full execution chain of a recent ICEDID sample in a detailed research paper hosted at Elastic Security Labs. In addition, we provide a comprehensive analysis of this malware sample and capabilities, including:

- Virtualization detection and anti-analysis
- C2 polling operations
- Shellcode execution methods
- Credential access mechanisms
- Websocket connections
- Installing a web browser proxy to capture all user traffic
- Reverse shell and VNC server installation
- Certificate pinning
- Data validation
- ICEDID observable TTPs
- Links to useful resources from Elastic

Detections and preventions

Detection logic

Preventions (source: https://github.com/elastic/protections-artifacts/)

- Malicious Behavior Detection Alert: Command Shell Activity
- Memory Threat Detection Alert: Shellcode Injection
- Malicious Behavior Detection Alert: Unusual DLL Extension Loaded by Rundll32 or Regsvr32
- Malicious Behavior Detection Alert: Suspicious Windows Script Interpreter Child Process
- Malicious Behavior Detection Alert: RunDLL32 with Unusual Arguments
- Malicious Behavior Detection Alert: Windows Script Execution from Archive File

YARA

Elastic Security has created multiple YARA rules related to the different stages/components within ICEDID infection, these can be found in the signature linked below:

Windows.Trojan.ICEDID

Elastic Security Labs is a team of dedicated researchers and security engineers focused on disrupting adversaries though the publication of detailed detection logic, protections, and applied threat research.

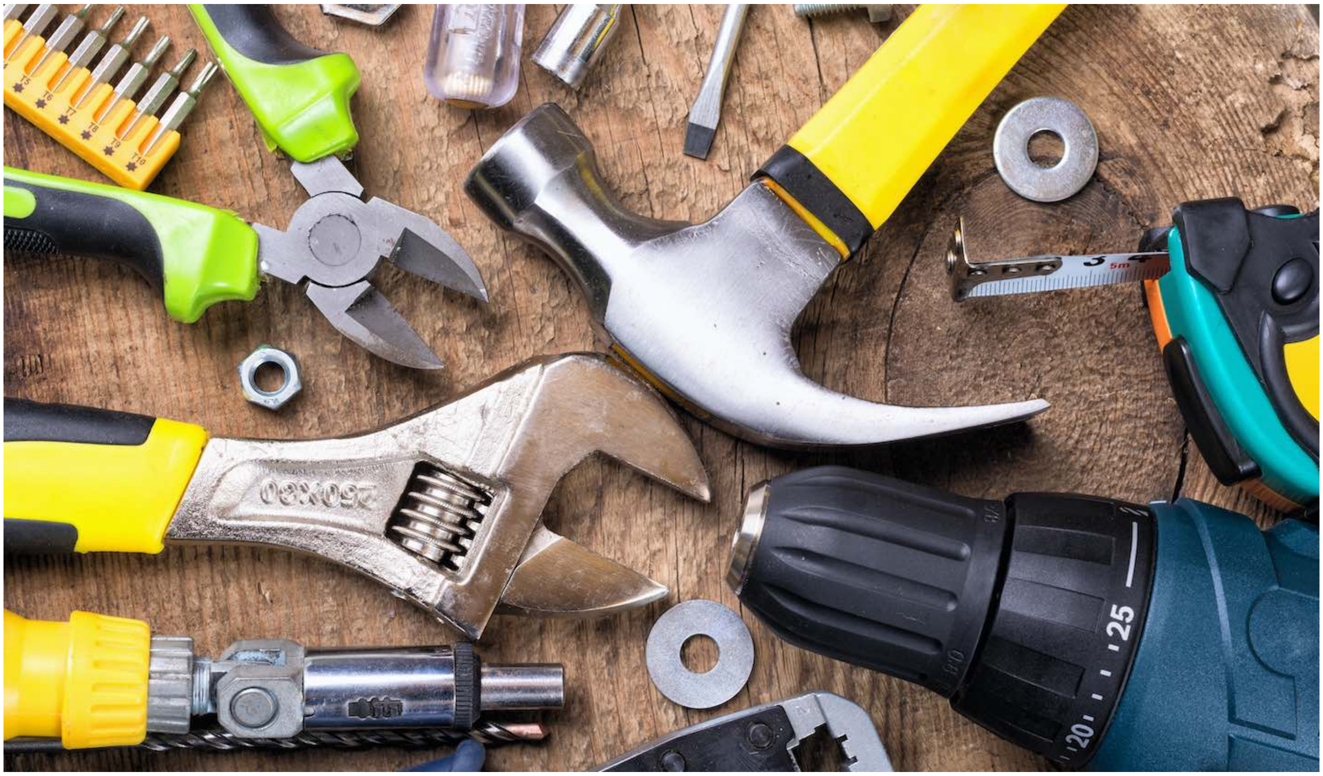
Follow us on @elasticseclabs or visit our research portal for more resources and research.

Related content

See all top stories

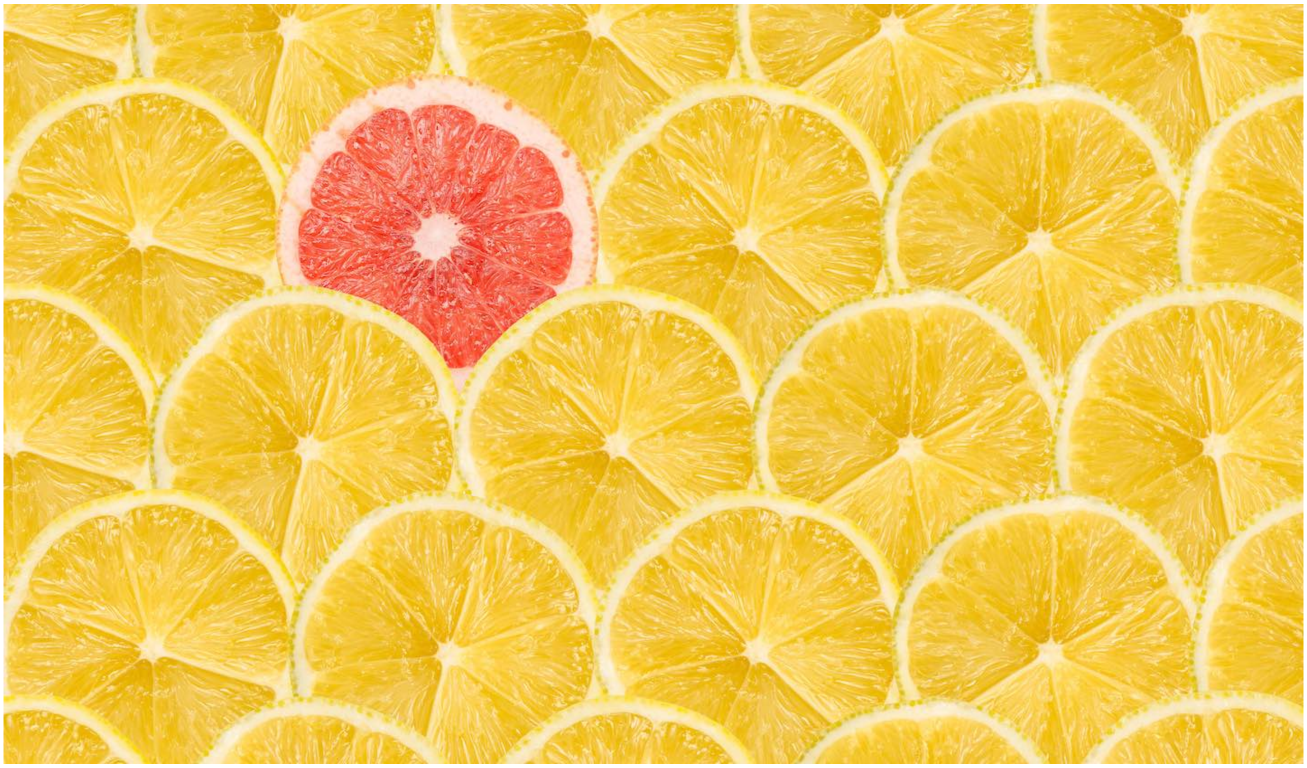
Elastic users protected from SUDDENICON’s supply chain attack

Elastic Security Labs is releasing a triage analysis to assist 3CX customers in the initial detection of SUDDENICON, a potential supply-chain compromise affecting 3CX VOIP softphone users.



Click, Click… Boom! Automating Protections Testing with Detonate

To automate this process and test our protections at scale, we built Detonate, a system that is used by security research engineers to measure the efficacy of our Elastic Security solution in an automated fashion.



REF2924: how to maintain persistence as an (advanced?) threat

Elastic Security Labs describes new persistence techniques used by the group behind SIESTAGRAPH, NAPLISTENER, and SOMNIRECORD.