Unveiling Olympic Destroyer: Impact and Implications

Scenario for 2024 CASP Cybersecurity Automation Village

Charlie Frick, Indicator of Behavior Sub-Project Chair

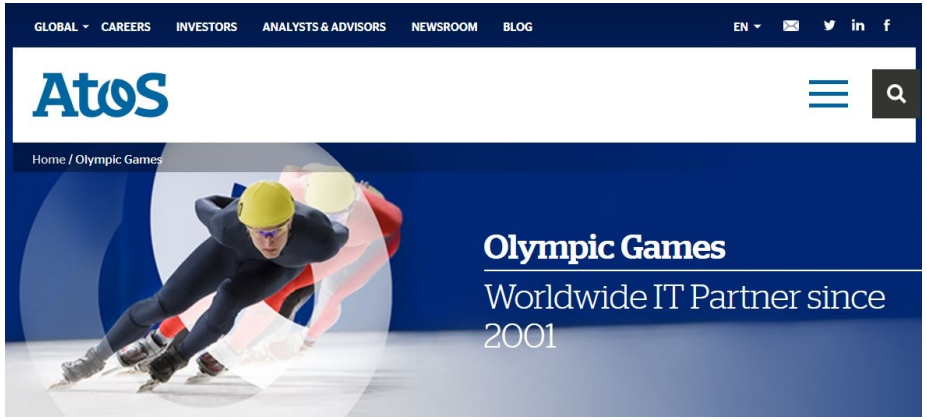
Acknowledgements to Jane Ginn, Jason Keirstead, David Bizeul, and the entire CASP project for their contributions

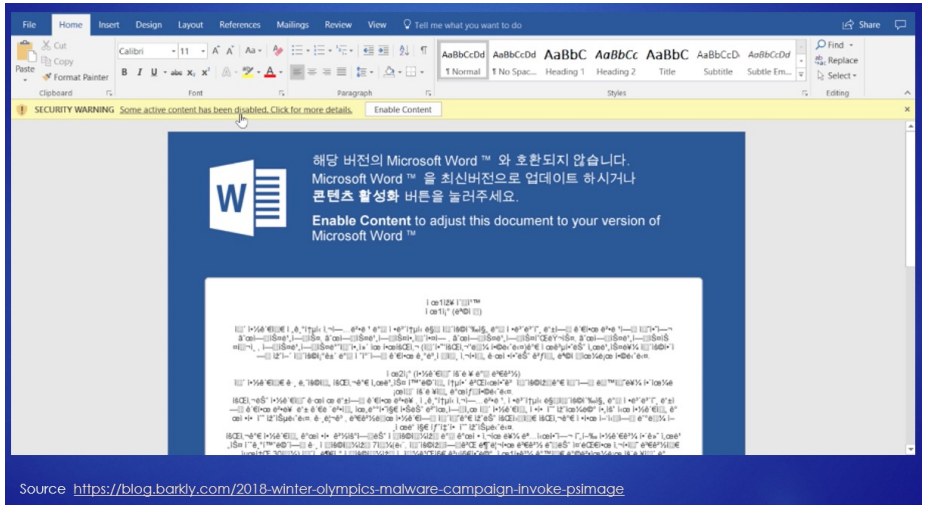
Background

- Cybersecurity Automation Village focuses on using open standards to foster rapid capability integration
- We need a common scenario to support the demonstrations throughout the event
- This talk will provide a high level overview of the scenario and some of the common elements used by several teams for the village

Olympic Destroyer (OD)

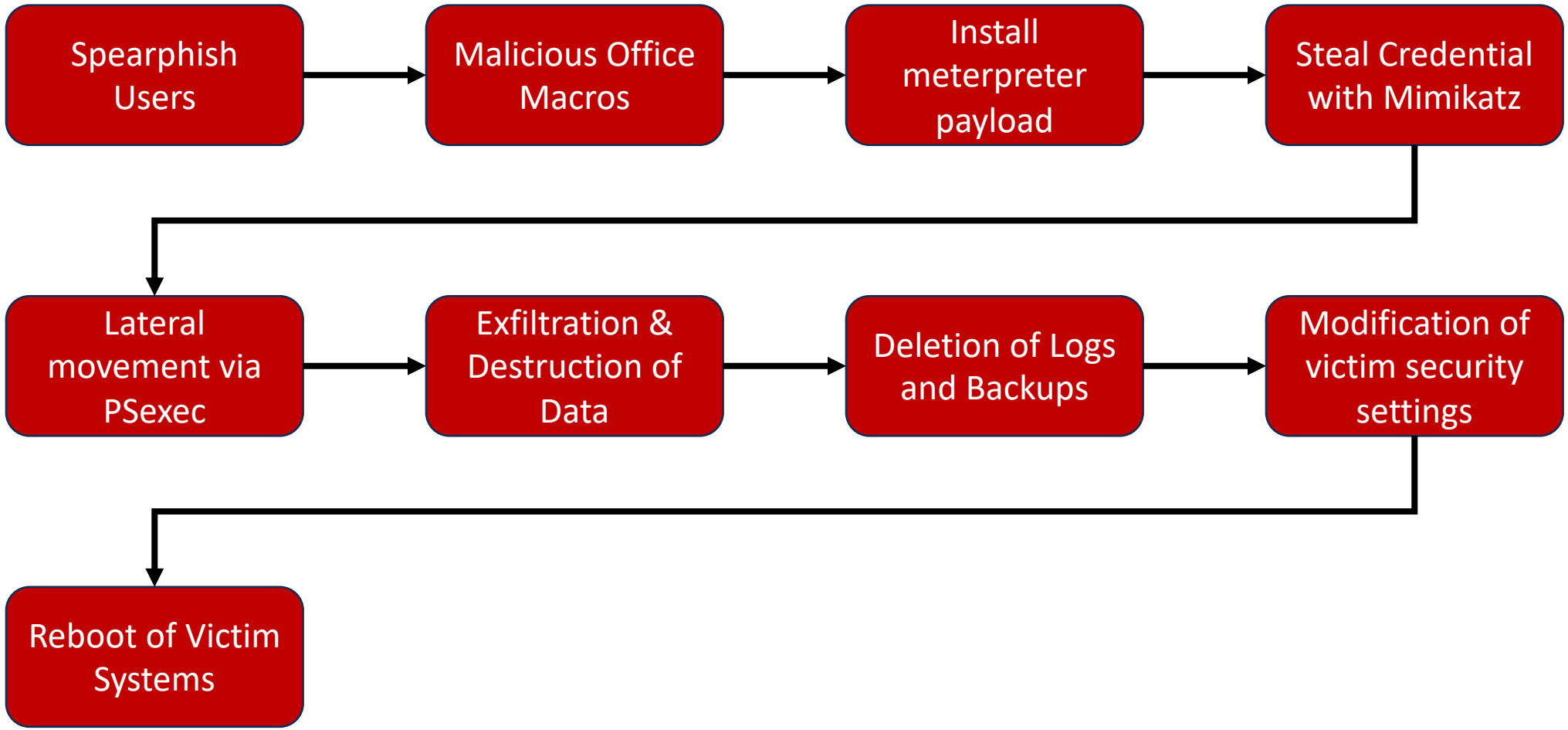
- Scenario for this year's village
- APT Campaign targeted the 2018 PyeongChang Winter Olympics
- Network worm
  - Propagated through Windows network shares
  - Stole passwords
  - Aimed to purge files and shut down infected systems





Source https://blog.barkly.com/2018-winter-olympics-malware-campaign-invoke-psimage

High Level Overview of OD Attack Workflow



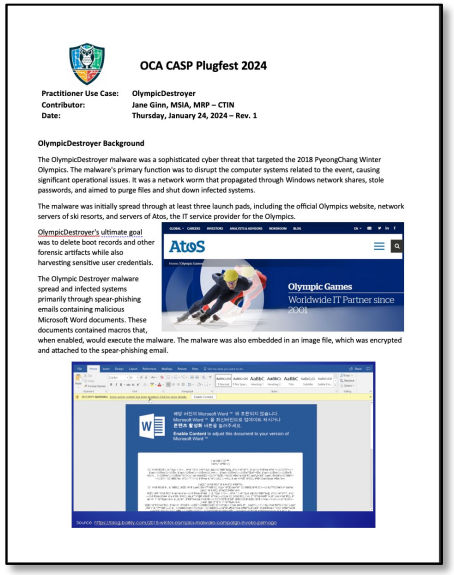
Common TTPs from OD Analysis

- Several common Tactics, Techniques, and Procedures were identified in the analysis of Olympic Destroyer Activity
- Several aligned with the MITRE ATT&CK framework
  - T1566.002 – Spearphishing Link
  - T1059.001 – PowerShell
  - T1134.001 – Token Impersonation
  - T1556.002 – Password Filter DLL
  - T1041 – Exfiltration over C2 channel
  - T1562 – Impair Defenses
  - T1485 – Data Destruction
  - T1529 – System Shutdown/Reboot

Contributions to Village

CASP Team Members provided data on OD to support this year's event

Threat Reports



OCA CASP Plugfest 2024

Practitioner Use Case: OlympicDestroyer
Contributor: Jane Ginn, MSIA, MRP – CTIN
Date: Thursday, January 24, 2024 – Rev. 1

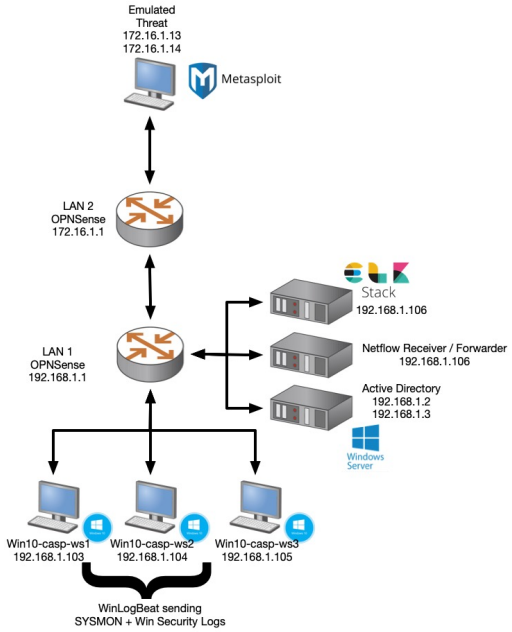
OlympicDestroyer Background

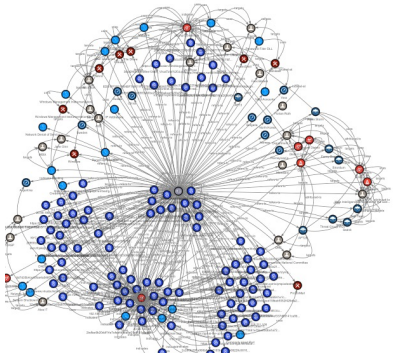
The OlympicDestroyer malware was a sophisticated cyber threat that targeted the 2018 PyeongChang Winter Olympics. The malware's primary function was to disrupt the computer systems related to the event, causing significant operational issues. It was a network worm that propagated through Windows network shares, stole passwords, and aimed to purge files and shut down infected systems.

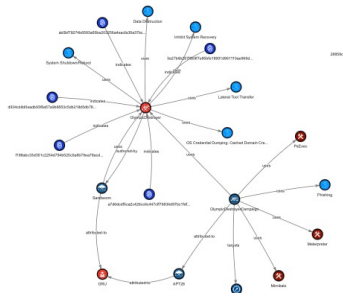
The malware was initially spread through at least three launch pads, including the official Olympics website, network servers of ski resorts, and servers of Atos, the IT service provider for the Olympics.

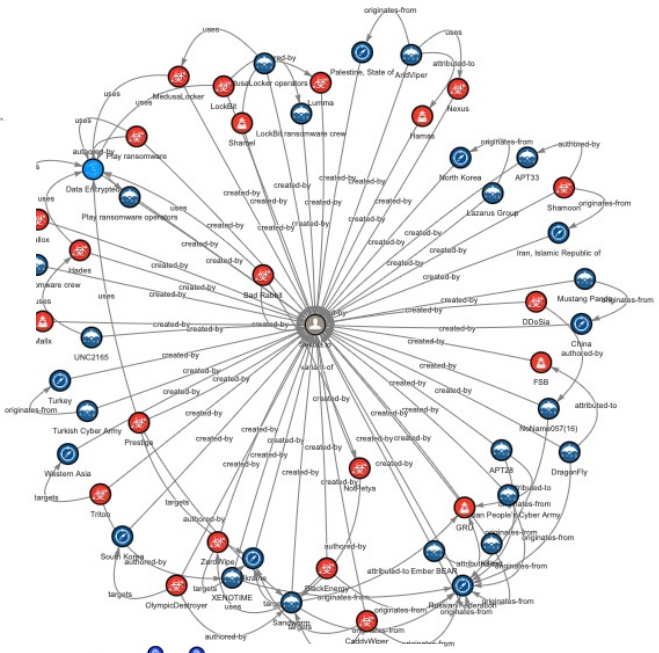
OlympicDestroyer's ultimate goal was to delete boot records and other forensic artifacts while also harvesting sensitive user credentials.

The Olympic Destroyer malware spread and infected systems primarily through spear-phishing emails containing malicious Microsoft Word documents. These documents contained macros that, when enabled, would execute the malware. The malware was also embedded in an image file, which was encrypted and attached to the spear-phishing email.

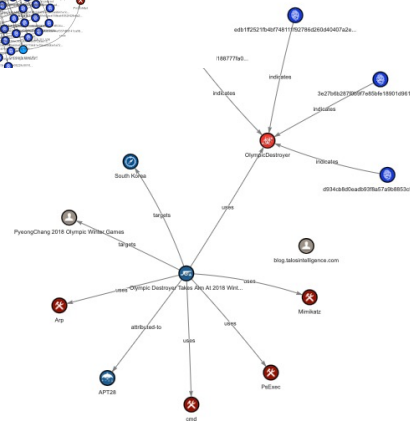


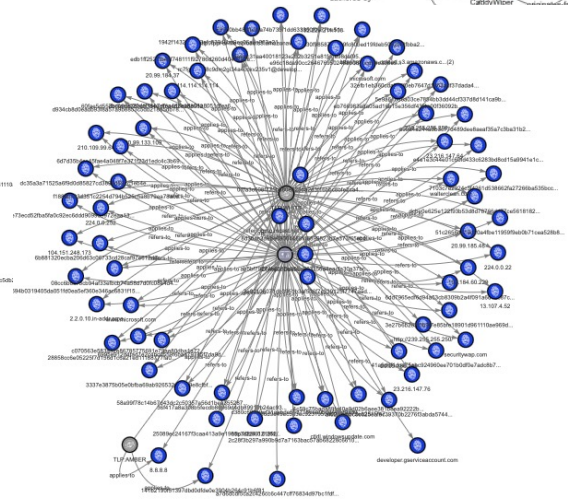






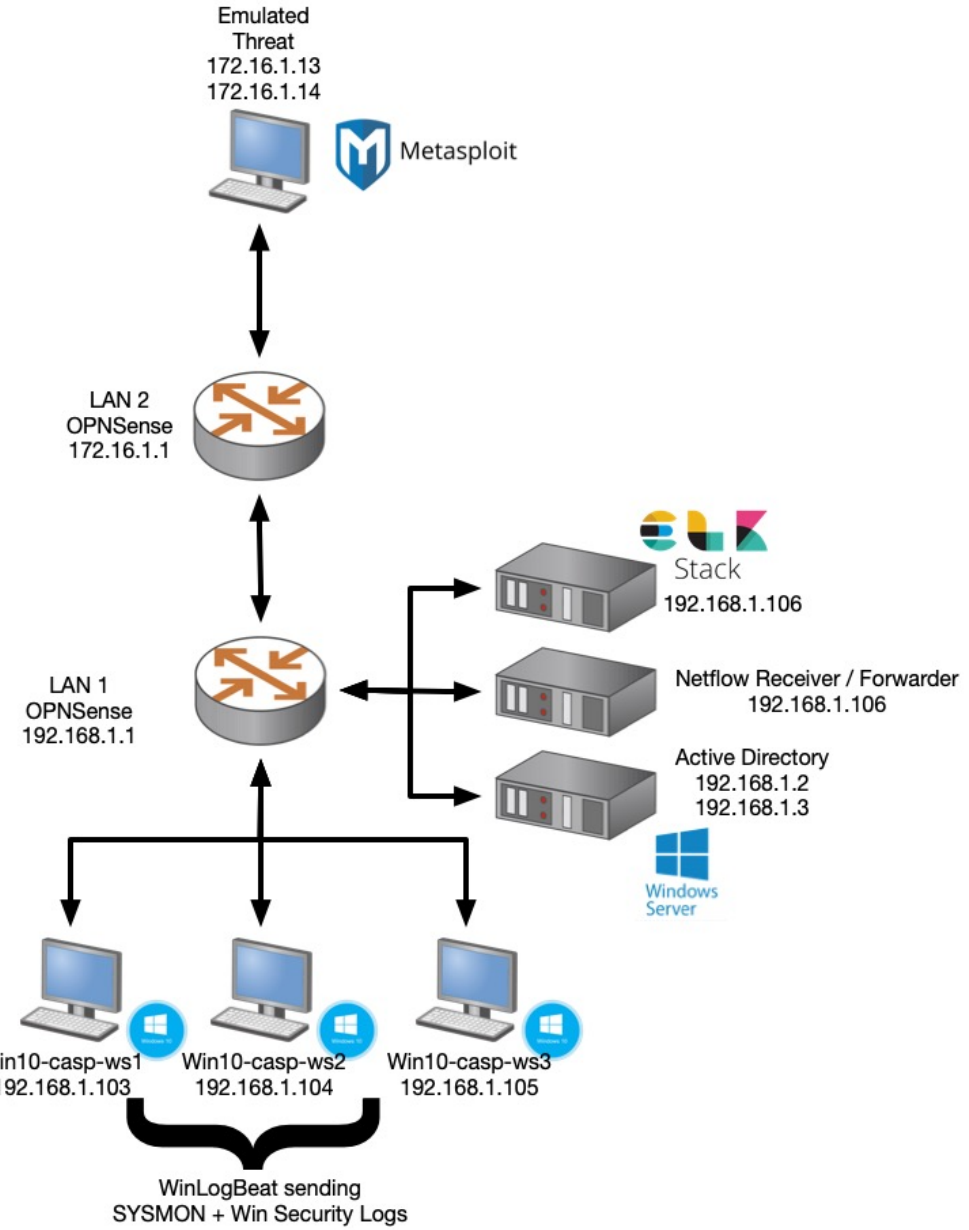
STIX Bundles





Emulated Threat

- Lab environment emulated OD attack
- Sysmon and Netflow logs were recorded
  - Logs were provided to CASP members
- Assisted in creation of
  - IOB Bundles
  - Stix-Shifter Detection analytics
  - Kestrel Huntbooks
  - CACAO response workflows



Conclusion

- CASP provides an excellent opportunity for the community to demonstrate the rapid integration capability of using open standards and tools
- Having a common scenario with technical artifacts allows plugfest members to rapidly build upon common elements
- Olympic Destroyer provides a realistic scenario that showcases the benefit of combining Cyber Threat Intelligence into security automation

Thank you to the entire CASP project for their contribution towards this year's plugfest