LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Intelligence Briefing Update NetSpectre

OVERALL CLASSIFICATION IS

UNCLASSIFIED

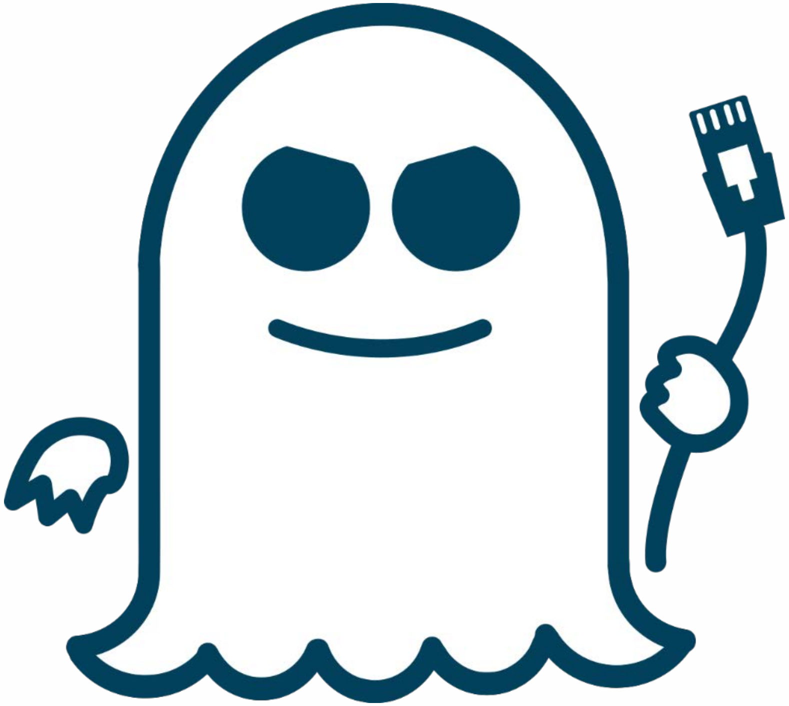
TLP:WHITE

8/2/2018

Agenda

TLP:WHITE

- NetSpectre
- Overview
  - Known Facts
- Proof-of-Concept
- Analysis
- Protection Recommendations
- Conclusions



Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

NetSpectre (infosecurity-magazine)

Background:

Spectre → *the initial disclosures*:

- Spectre tricks a target process into performing a sequence of memory accesses which leak secrets from chosen virtual memory locations to the attacker.
- Required an attacker to be able to run code of their choosing on a victim system

The vulnerability:

- Spectre manipulates the branch prediction
- Completely breaks confidentiality and renders virtually all security mechanisms on an affected system ineffective

What was vulnerable:

- Browsers → suitably crafted JavaScript could be used to perform Spectre attacks
- Cloud hosts
- **Outside of Browser and Cloud Hosts, impacts were limited**

Overview

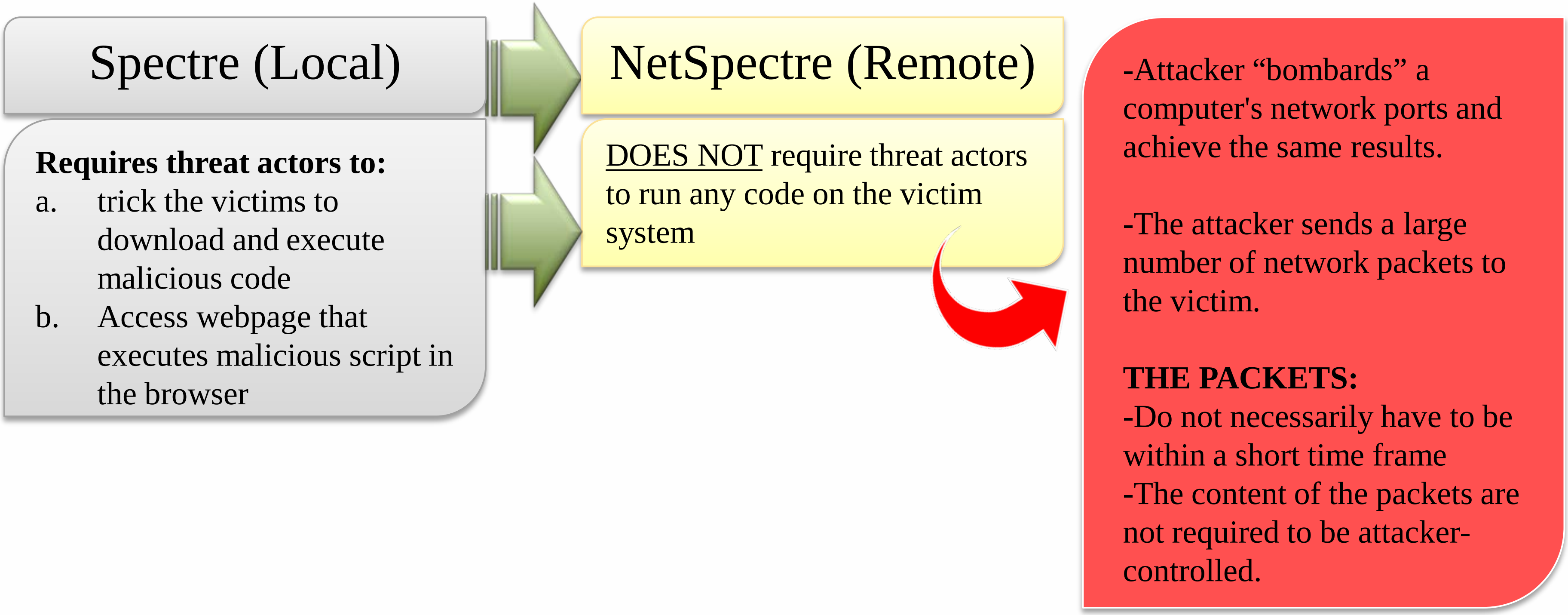
NetSpectre (misc0110)

- “The first remote Spectre attack” → attacks via network connections
- Could allow an attacker to read/steal arbitrary memory via network connections
- Slow exfiltration speed reportedly:
  - 15 bits/hour for attacks carried out via a network connection and targeting data stored in the CPU's cache.
  - Academics achieved higher exfiltration speeds → up to 60 bits/hour
  - **Note: speeds expected to increase in the future
- Sending a large amount of specially crafted (malicious) packets to a target host

Overview

Spectre VERSUS NetSpectre (misc0110)

- **Comparison:**



Spectre (Local)

Requires threat actors to:

a. trick the victims to download and execute malicious code

b. Access webpage that executes malicious script in the browser

NetSpectre (Remote)

DOES NOT require threat actors to run any code on the victim system

-Attacker "bombards" a computer's network ports and achieve the same results.

-The attacker sends a large number of network packets to the victim.

THE PACKETS:

-Do not necessarily have to be within a short time frame

-The content of the packets are not required to be attacker-controlled.

Protections

Mitigation

- NetSpectre attacks can be prevented using the mitigations recommended for the original Spectre
  - NetSpectre is related to Spectre variant 1 – CVE-2017-5753
  - This patch, in theory, should apply to NetSpectre

- Because NetSpectre is a network-based attack:
  - Network-layer countermeasures can also be efficient in blocking this threat
  - DDoS protection will block the high volume of malicious packets

Conclusion

Upcoming Briefs

- Trends in Malicious Macro Usage
- Cryptomining Landscape
- Various APT/FIN Groups

Analyst-to-analyst webinars are available

Questions / Comments / Concerns?

HHS HCCIC Email Address: HHSHCCIC@hhs.gov