Ransomware

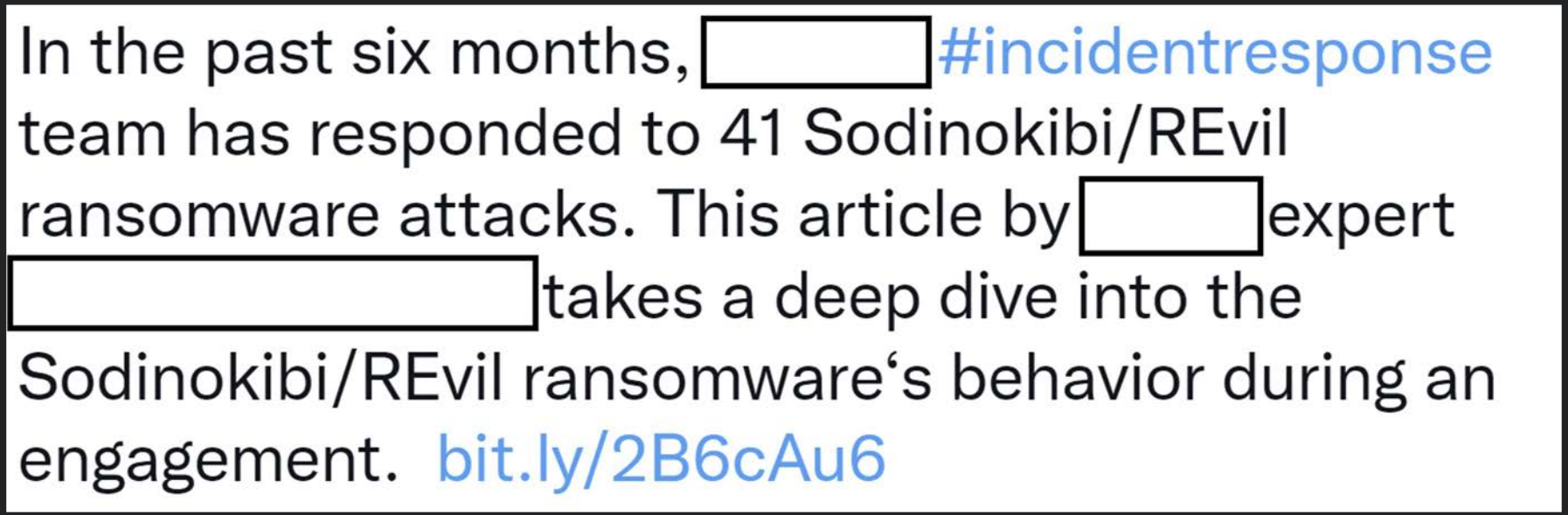
We need to stop focusing on the EXE

HUNTRESS

whoami

Where We Are Now

Open reporting tends to focus on the final EXE…



HUNTRESS

Where We Are Now

- 12 Aug - Crowdstrike publishes “Anatomy of the Wiper Malware, pt I”
  - Presented techniques used in “wiping”, but ***not*** how the malware gets deployed

However…

- 10 Aug - Cisco Talos publishes details of attack suffered
  - Complete walk-thru, for initial access
  - Included commands, TTPs

Where We Are Now

- 25 Aug - Trend Micro report on “Agenda” ransomware
  - Report states that the malware “targets” victims, “customizes” attacks
  - Report references “one incident”, accessing Citrix server via use of “valid account”
  - Nothing beyond that…no reference to IAB

Use of “ransomware” is synonymous with “threat actor” or “RaaS provider” - ***no distinction***

Where We Are Now

Not focusing on intrusion intel has us…

- Still getting attacked
- Still detecting attacks *after* file encryption
- Still submitting insurance claims

What about ***Control Efficacy***?? Detections?

Impacts

- RaaS + IABs
- Insurance carriers/breach coaches
  - Actuary data for policy creation
  - Guidewire “Hiding in Plain Sight” white paper by Erin Kenneally
  - Add’l content from Daniel Woods, etc.
- Legal Counsel
- DFIR Consulting Firms
  - Better understanding of attack cycle, TTPs, behaviors
  - Utilization Business Model

We *CAN* Talk About These Things

- Anonymize through aggregation - no need to share customer info
  - Samas - 2016
- MITRE ATT&CK Heat Maps ***with*** Observables (CS GTR 2019, 2020)
- TTPs/behaviors, including sequence, timing, variations, etc.
- All lead to
  - Attribution
  - Actuary
  - Better controls

Wrap Up & Q/A

Harlan Carvey

harlan.carvey@huntresslabs.com

HUNTRESS

Thank You

u/huntresslabs

huntress-labs

@HuntressLabs

@huntresslabs

huntress.com/blog

HUNTRESS