redsense
INTELLIGENCE OPERATIONS

TLP:WHITE

PUBLICATION DATE: DEC 7 2022

Holidays Routine 2022/23: Not Novel

Naughty or nice, there's a few things in cyber circuits that won't change in this year's Holiday Season.

1. Threat actors are financially motivated, driven by human needs, and the holidays are expensive
2. Threat actors stereotypically choose simple solutions available for their problem space(s)
3. Unmanaged digital disarray carries potential for breach consequences

Threat actors are also creatures of habit, often leveraging shared TTPs and re-used services and infrastructure, which gives defenders a significant potential advantage. Take for instance the 'not novel' tactics recently employed by recent ransomware campaign for Daixin, Hive, and Cuba.

T1078 – Valid Accounts
T1133 – External Remote Services
T1190 – Exploit Public Facing Applications
T1566 – Phishing
T1598 – Spearphishing Attachment
T1059 – Command and Scripting Interpreter
T1537 – Transfer Data to Cloud Account

Infrastructure and service reuse are commonly observed in many of these campaigns also, e.g., examine the recent Cuba indicators of compromise (IOCs) against other published threat research indicators.

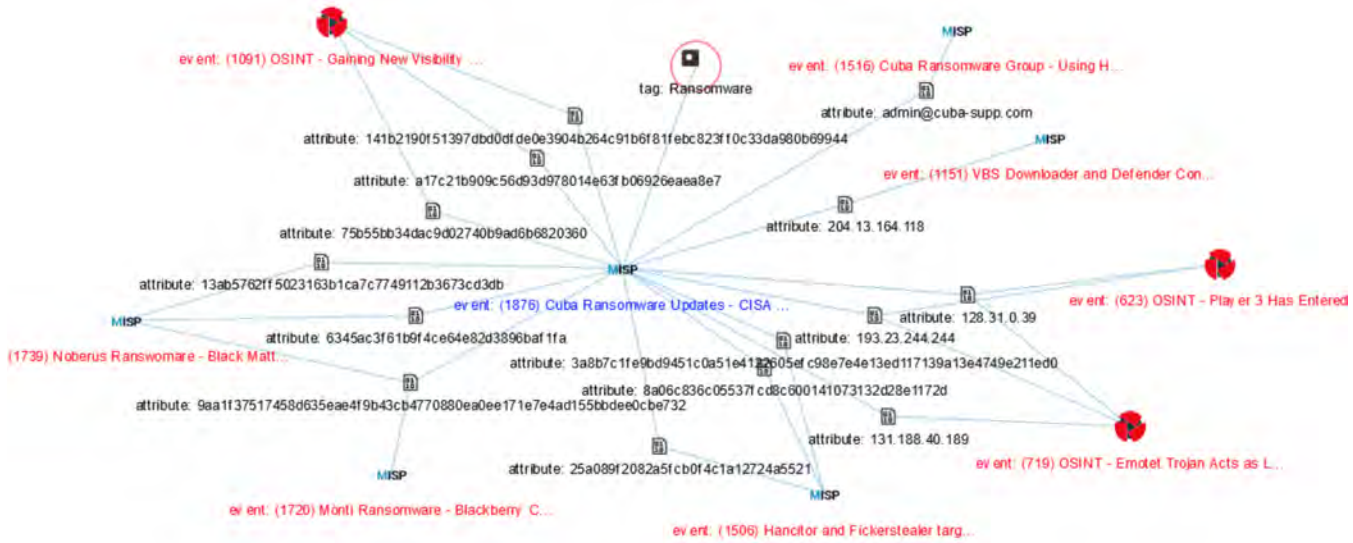

figure 1. Cuba ransomware indicators and connections

Proper organizational security awareness, posture, controls, and other relevant precursors are worth their weight in gold this Holiday season.

Phishing Campaigns

November has demonstrated closer linkages between malspam delivery, initial infections/accesses, and ransomware delivery. Whether it be indications of Emotet's close relationship with the Quantum, or Qbot deliveries leading to Black Basta deployments, the tightening of operations observed certain elements of the crimeware ecosystem is notable.

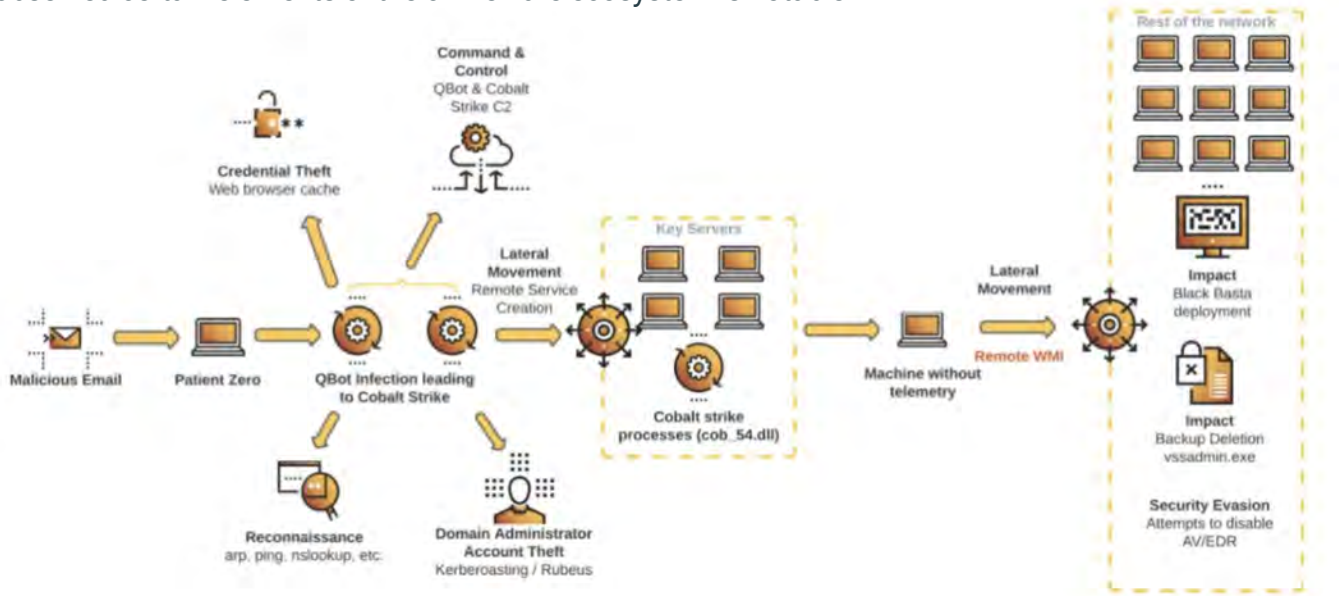

figure 2. QBot infection leads to Black Basta

Established controls around embedded links and attachments remain somewhat effective, especially when there is detection context around/for spoofed SPF headers, compromised sites, newly registered/resolving domains, etc.

Phishing training here should mimic adversarial campaigns to include advances in social engineering (e.g., fake invoice to lure victims to call centers), should emphasize OPSEC fundamentals.

Application Exploitation

Still shell shocked from last year's Log4J scenarios? Between recent Apache Commons Text exposure and ongoing threat of supply chain attack, it's another hectic holiday season for security practitioners tracking known vulnerabilities exploited in the wild.

Exposed (potentially vulnerable) devices are the gift that keeps on giving this year. Recent reporting by Microsoft calls additional concern to what ICS communities have been tracking for months, a probable wave of supply chain attacks relating leveraging exposed IoT devices and popular SDKs used in 'System on Chip' firmware implementations (e.g., RealTek's CVE-2021-35395, and CVE-2022-27255).

The Shodan screengrab below relates to ~1.5M Internet exposed Boa web servers. Understanding the vulnerabilities (e.g., CVE-2017-9833, CVE-2021-33558, and follow-on RCE) of these 200,000+ U.S. based Boa webservers and the potential therein for adversarial access, lateral movement, etc. is critical for potentially affected organizations.

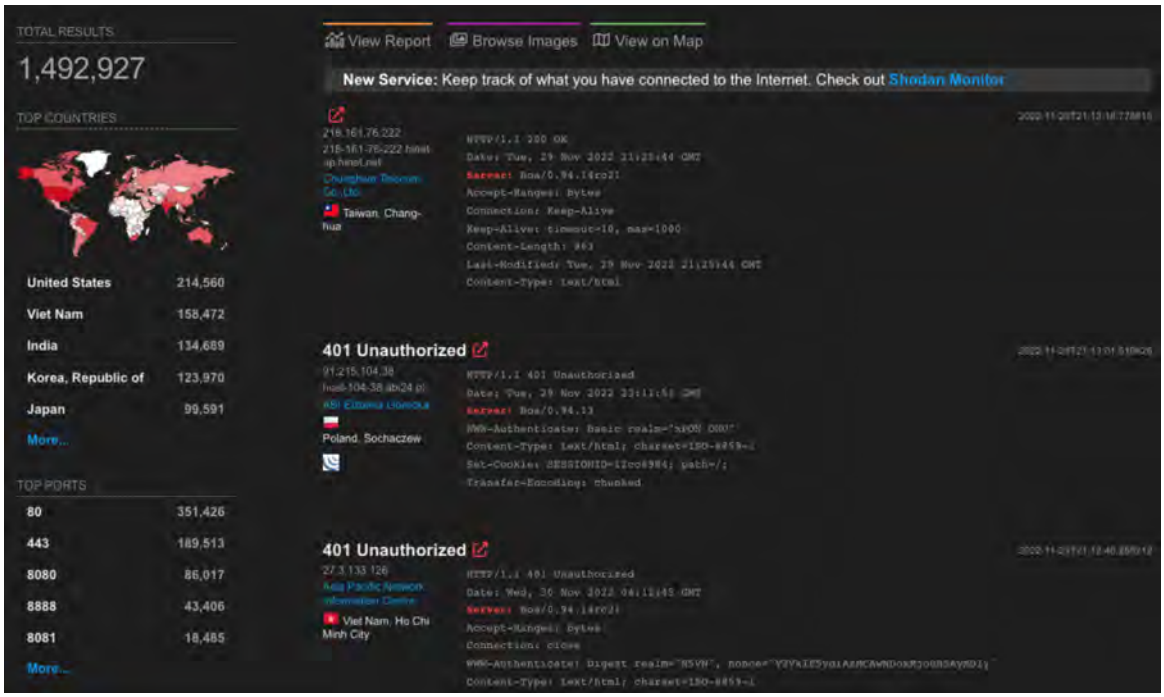

figure 3. Shodan query against Boa web servers

Perhaps not always glamorous, organizational controls for asset inventory, governance, and monitoring related controls remain paramount.

Social Media Unraveling?

Along with email, many organizations have taken to social media outlets for much of their brand and marketing needs and, in some cases, even patient outreach. Unfortunately, several popular 'business approved' social media outlets have suddenly become a volatile risk factor for this Holiday season.

In recent weeks, reeling digital giants Meta and Twitter have both been impacted by ongoing and substantial data breach/spill scenarios.

figure 4. Meta leaks half a Billion users private info

Reliance upon and now potential disruption(s) of these 'trusted services' is forcing legitimate social media campaigns to adjust, which incurs additional risk for not just social engineering and related adversarial action, but also the risk of vulnerabilities (e.g., 'Warning – do not use Hive social') and misconfigurations as they pivot to new social media platforms. For example, Novant Health exposed 1,362,296 individuals sensitive information via a Meta Pixel ad tracking script. (Ref: BleepingComputer)

Password Policies and Multi-Factor Authentication (MFA)

If you're reading this and wondering if you should enable better password policy controls or MFA, the answer is a resounding 'YES'. Time and time again, Red Sense observations have verified the efficacy of competent and appropriate security controls. (Ref: CISA's guidance for MFA)

During the fall-winter of 2022, Red Sense observed multiple healthcare organizations victimized by threat and ransomware actors due to simple failures in password and MFA policies and/or implementations.

figure 5. Sample poor passwords (compromised)

Compromised credentials also remain reliable attack vector for adversaries this Holiday season. Credential thieves running RedlIne, Raccoon, Vidar, Borwita, Meta, etc. raise proverbial eggnog as they hold Holiday vigil alongside all of the Work-From-Home (WFH) employees (potential victims).

Britton White and PogoWasRight.org have created a free handout about some of the risks of storing passwords and in browsers and browser extension apps.

figure 6. Redline article sourced to pogowasright.org

Conclusion and Recommendations

While security seems 'Heightened' for every Holiday season lately, take some solace in the fact that proper organizational security (awareness, posture, controls, and resourcing) will keep you safer (and likely less stressed) this year.

Additionally, after analyzing dozens of ransomware actors and campaigns this year, the prioritization of several detection approaches and methods are recommended:

External Connections and Access:

- Prioritize network detection(s) around external connected services, standard ports, etc.
- Stop LAN protocols such as NetBIOS and SMB from direct exposure to the Internet
- Investigate all heavy HTTPS outbound to infrastructure and cloud services (e.g., Digital Ocean)

Remote Administration Tools

- 3P Governance and detection around approved remote desktop applications
- Block unapproved remote applications, services, etc. (e.g., Anydesk, Atera, TeamViewer)
- Prioritize network detection(s) around remote connections, standard ports (e.g., 3389), etc.

Critical WIN Patching/Logging:

- Embrace the patch Tuesday cycle
- Event ID 4698 – Scheduled Task Creation (Persistence) logging is NOT enabled by default in enterprise environments
- Event ID 4688 – New Process Creation logging + Command Line Process Auditing
- Detect/Investigate applications commonly used maliciously, e.g., PowerShell, WMI, etc.

Stay safe this Holiday season!

ABOUT US

Red Sense, LLC is a veteran-owned small business (VOSB), that monitors and tracks significant events and forces within the Security space in order to provide our customers with deep insight into the myriad of new technologies, threat actors, software vulnerabilities and exploits, and sometimes suspect vendor sales pitches. RedSense offers vendor-agnostic and objective counsel to help address the evolving Security and Intelligence spaces.