kindred

Security Newsletter

23 September 2019

Subscribe to this newsletter

NCSC Cyber Threat Trends Report: Analysis of Attacks Across UK Industries

The United Kingdom's National Cyber Security Centre (NCSC) recently released their Incident trends report (October 2018 – April 2019) which highlights some of the trends seen across various UK government entities, organizations, and sectors.

The first thing the NCSC chose to highlight in their report was the observed attacks against Office 365, Microsoft's cloud services suite. According to Microsoft, there are over 155 million Office 365 business users as of 2018, a massive attack surface for a single service. When you combine that with the fact that passwords get reused all the time—maybe even for Active Directory integration (O365 makes this easy for Windows users for obvious reasons)—it's no wonder threat actors see it as an appealing target.

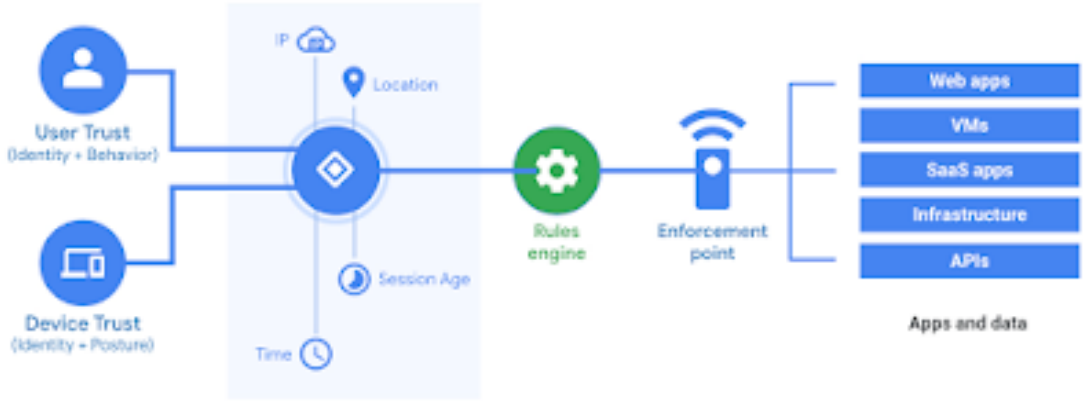
Ransomware isn't going away. Seemingly every day, there's a new report that a small municipality in the United States has been hit, with demands reaching the millions of dollars. The UK isn't immune to this either. As the NCSC report points out, Ryuk, LockerGoga, and BitPaymer have all been fairly prevalent over the time period. Additionally, the Emotet, TrickBot, and Dridex botnets have all been seen being used as delivering ransomware once installed on the machines. If there was any doubt that botnets aren't being used for MUCH more than denial of service attacks, rethink your assumptions.

Last, supply chains are being attacked by nation-state threat actors such as APT10, as well as cybercriminals looking to monetize their attacks, like the operators of GandCrab. It's important that supply chain partners are evaluated and held to the same security standards as the companies themselves. That partner's access may make them an attractive target.

Read More on DigitalShadows

Incident trends report (October 2018 - April 2019)

How Google adopted BeyondCorp: Part 3 (tiered access)



This is the third post in a series of four, in which we set out to revisit various BeyondCorp topics and share lessons that were learnt along the internal implementation path at Google.

By separating trust from identity, we can define infinite levels of trust, if we so desired. At any point in time, we can define a new trust level, or adjust existing trust level requirements, and reevaluate a device's compliance. This is the heart of the tiered access system. It provides us the flexibility to define different device trust criteria for low sensitivity applications from those used for high trusted applications.

At Google, we initially supported four distinct tiers ranging from Untrusted to Highly-Privileged Access. The extremes are easy to understand: Untrusted devices should only access data that is already public while Highly-Privileged Access devices have greater privilege internally. In our current model, the vast majority of devices fit in one of three distinct tiers: Untrusted, Basic Access, and Highly-Privileged Access.

In the next and final post in this series, we will discuss how we migrated services to be protected by the BeyondCorp architecture at Google.

Read More on Google Security Blog

Read part 2 (devices)

Read part 1

More #News

- Two Widely Used Ad Blocker Extensions for Chrome Caught in Ad Fraud Scheme
- Magecart strikes again: hotel booking websites come under fire
- iOS 13 Passcode Bypass Lets You View Contacts on Locked Devices
- Eight US Cities See Payment Card Data Stolen
- Phishing Attack Targets The Guardian's Whistleblowing Site

- Phishing Attack Targets The Guardian's Whistleblowing Site
- Misconfigured Google Calendars Share Events With the World
- Database leaks data on most of Ecuador's citizens, including 6.7 million children
- GitHub Becomes CVE Numbering Authority, Acquires Semmle
- Snowden Says He Would Return to US If He Can Get a Fair Trial
- Banks, Arbitrary Password Restrictions and Why They Don't Matter
- Millions of Lion Air Passenger Records Exposed and Exchanged on Forums
- Microsoft Phishing Page Sends Stolen Logins Using JavaScript
- 200,000 Sign Petition Against Equifax Data Breach Settlement
- 400 Million Medical Radiological Images Exposed on the Internet
- MITRE Publishes New List of Most Dangerous Software Weaknesses

#Patch Time!

- LastPass Patches Bug Leaking Last-Used Credentials
- VMware Patches Six Vulnerabilities in Various Products
- Server-squashing zero-day published for phpMyAdmin tool
- Update Google Chrome Browser to Patch New Critical Security Flaws
- Critical Bug In Harbor Container Registry Gives Admin Access
- Windows Defender malware scans are failing after a few seconds
- Before He Spammed You, this Sly Prince Stalked Your Mailbox
- Remote access flaws found in popular routers, NAS devices
- Code Execution Vulnerabilities Found in Aspose PDF Processing Product

#Tech and #Tools

- Shhmon — Silencing Sysmon via Driver Unload
- Sooty: The SOC Analysts all-in-one CLI tool to automate and speed up workflow.
- How Google adopted BeyondCorp: Part 3 (tiered access)
- Writing a File Monitor with Apple's Endpoint Security Framework
- Forcepoint VPN Client for Windows - Unquoted Search Path and Potential Abuses (CVE-2019-6145)
- Security: HTTP Smuggling, Apache Traffic Server
- Abusing VPC Traffic Mirroring in AWS
- Vulnerable SSO Project
- Invoke-SocksProxy: local or "reverse" Socks proxy using powershell
- Lastpass: bypassing do_popupregister() leaks credentials from previous site
- CURRYFINGER - SNI & Host header spoofing utility
- If you're not using SSH certificates you're doing SSH wrong
- MISP improved model to expire indicators based on custom models

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. Kindred is one of the largest online gambling companies in the world with over 26 million customers across 100 markets. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 26 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us