Borderless Threat Intelligence
Proactive Supply Chain Monitoring for Signs of Compromise

Jason Trost
Nicholas Albright
Feb 4th, 2016
whoami

Jason Trost

• VP of Threat Research @ ThreatStream
• Previously at Sandia, DoD, Booz Allen, Endgame Inc.
• Background in Big Data Analytics, Security Research, and Machine Learning
• Big advocate and contributor to open source:
  • Modern Honey Network, BinaryPig, Honeynet Project
  • Apache Accumulo, Apache Storm, Elasticsearch
whoami

Nicholas Albright

- VP of Security and Intelligence @ ThreatStream
- Previously at VMware, Department Of Interior, Consultant for Fed/Financial
- Old School Hacker, Penetration Tester, Tactician and Puzzletier.
- Currently focused on Sinkholes, Darknets and Malware
ThreatStream

• Cyber Security company founded in 2013 and venture backed by Google Ventures, Paladin Capital Group, Institutional Venture Partners, and General Catalyst Partners.

• SaaS based enterprise security software that provides actionable threat intelligence to large enterprises and government agencies.

• Our customers hail from the financial services, healthcare, retail, energy, and technology sectors.
Agenda

• Background
• Supply Chain Monitoring
• Suspicious Domains
• Network Cleanliness
• Social Media and DarkWeb
• Credential Exposures
• Wrap up
Background
Defining your Supply Chain

Your supply chain will be Unique

- Financial records
- Earnings Reports
- Payroll

- Power and Utilities

- Environmental Control
  and Critical Suppliers

- Software, Third Party
  Libraries, Remote Access
  Tools (VPN)

- Supplier Inventory
- Technical Component Inventory
- Vendor Assessments

- Contractors and
  Workforce
Threat Intelligence

- Also, One Size Fits One

How can you use Your Threat Intelligence solution to identify Supply Chain Threats?
How do I?

On Premises Controls will only work for supply chain events within your network
- Code / Library Reviews
- Network Flow and Account Access Reviews
- Internal Pivoting
- Threat Feeds (Your Organization on Block lists, Bad guys accessing your org)

Zero Premises Controls will extent your capabilities deep within your suppliers infrastructure!
- Public Credential Exposures (Yourself, Partners, Suppliers)
- Threat Feeds (External Organizations on Block lists)
- Shodan/Censys Reviews
- Suspicious Domain Registrations (Yourself, Partners, Suppliers)
- Social Media Monitoring
Supply Chain Threat Intelligence

Document and Research:
• Supply chain company’s security posture?
  • Network cleanliness?
  • Web footprint? (Services/Capabilities)
• Supply chain company compromised?
  • May put you at risk
  • How Recent?
  • Repeated?
• Supply chain company’s brand used to phish you?
  • Pay Special Attention to Service Desk Services!
• Supply chain company being targeted?
  • Examples may not be so obvious
    • DNS Registrars hold the keys
Suspicious Domain Name Monitoring

- Adversaries register domains mimicking your brand or your supply chain’s brand
  - Typosquat, Homoglyph, Character Omission/insertion/swap, etc
  - Deceptive domains: vpn-mycompany.com, portal-mycompany.com
- Used to phish you or as C2 domains
- Very effective social engineering tactic

- **Data Sources:** New Domain registrations, Passive DNS, Virustotal Hunting, URLCrazy
- **Operations:** SIEM integration, Email alerts, IDS Signatures, DNS RPZ
Examples

threatstream.com
threastream.com
threatsrream.com
threatstr3am.com
threatstr3gm.com
threatsyyzeam.com
thpeastream.com
threatstteam.no
threatststream.us
threatstrwam.com
threatstrteam.org
threatststreamcm.com
threatwtream.com
threatstream.ca
threattrgam.com
threatsstrteam.com
threatatream.com
threatstream.com
threastream.com
threatstream.ch
threatstream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
thvreastream.com
Don’t Forget About Dynamic DNS

threatstream.lioha.com
threatstream.meibu.net
threatstream.kz.com.ru
threatstream.gnway.cc
threatstream.ircop.cn
threatstream.igirl.ru
threatstream.newsexstories.com
threatstream.free-stuff.com.ru
threatstream.leedichter.com
threatstream.ggsddup.com
threatstream.yooky.com.ru
threatstream.za.pl
threatstream.servercide.com
threatstream.sxn.us
threatstream.wmdshr.com
threatstream.gnway.net
threatstream.rincondelmotor.com
threatstream.pluginfree.net
threatstream.estr.com.ru
threatstream.teksunpv.com
threatstream.gameyg.com
threatstream.redbirdrestaurant.com
threatstream.linkpc.net
threatstream.support-microsoft.net
threatstream.openoffcampus.com
threatstream.keygen.com.ru
threatstream.cu.cc
threatstream.pornandpot.com
threatstream.informatix.com.ru
threatstream.fuentesderubielos.com
threatstream.9wide.com
threatstream.jaqan.cn
threatstream.hyfitech.com
threatstream.easyeatout.com
threatstream.xicp.cn
threatstream.xenbox.net
threatstream.publicvm.com
threatstream.ven.bz
threatstream.meibu.com
threatstream.ag.pl
threatstream.m3th.org
Case Study: Suspicious Domain Registration

• Abuse isn’t always about network compromises
• Major US Based Cable and Telecommunications company
• Fraudulent procurement attempt
• Email sent from ${user}@${company}-us.com, but with the correct letter head and markings
• Discovered by SIEM scanning incoming email logs and flagged messages as suspicious
• Security team prevented fraudulent transaction, fraud team seized domain
Network Cleanliness Monitoring

• Systems from your IP space or your supply chain’s showing up as ...
  • Bot IPs
  • Scanning IPs
  • Brute force IPs
  • Spam IPs
• Your webserver hosting malicious content?
• Vulnerable or unexpected services running and discoverable?

• **Data Sources:** Threat intelligence feeds, honeypot events, botnet sinkhole, Portscan/Web crawl data
• **Operations:** SIEM integration, Email notifications
Case Study: Network Cleanliness

• Large Hi-tech firm evaluating IT staffing company for outsourcing some development and IT services
• IT Staffing company would need VPN access and access to our internal IT resources
• Passive vendor audit performed using threat intelligence data and public portscan repository
• Upon inspection, IT staffing company had very poor network hygiene
  • tens of IPs regularly checked in to malware sinkholes
  • tens of IPs regularly scanned honeypot sensors
  • thousands of compromised credentials
• IT staffing company deemed too risky
Social Network and Darkweb Monitoring

• Are you are your supply chain being discussed as a target on social media or the darkweb?
• Public Threats made?
• Malicious software purpose built to target your company or your supply chain?
• “Babylon” Darkweb Forum Posting on Healthcare Orgs Supply chain vendors to target

Posting from the Hell Darkweb forum
Case Study: Social Media/Darkweb Monitoring

- Brand monitoring for Major US Based Retailer
- Discovered a custom built attack tools designed for the sole purpose of brute forcing a specific part of the retailer’s web application
- Provided the sample and a report about what it did, how it worked and who built it to the retailer
Credential Exposure Monitoring

- Bulk Usernames and passwords exposed
- Usually not your company or supply chain directly exposed
- Usually 3rd party sites, but your employee email addresses are used, passwords likely reused

- Data sources: Paste sites, Google Dorks, Darkweb
- Operations: SIEM integration / orchestration system – notify users/reset passwords, Email alerts
- Multifactor Authentication not used enough

![Credential Exposures](chart)
Case Study: Credential Exposures

• Brand monitoring for a Major Food and Beverage Company
• Discovered leaked credential exposure from an internal IT wiki page that was accidently exposed
• Company alerted and changed all passwords within 24 hours
• No evidence that these credentials were abused in that time
Take Away: Inventory

• Step one is create an inventory of yourself and critical supply chain partners
• The adversaries this, you should too

• Email domains
• Personal email addresses of key executives
• IP address space
• brand names
• external domain names
• internal domain names
## Take Away: Operationalizing

<table>
<thead>
<tr>
<th>Data Sources</th>
<th>Operationalizing</th>
</tr>
</thead>
</table>
| **Suspicious Domains** | • New domain registration data  
  • Passive DNS  
  • Virustotal Hunting  
  • Repeated reviews of DynDNS | • SIEM integrations  
  • Email based alerting |
| **Network Cleanliness** | • Honeypots / C2 Sinkholes  
  • Open source threat feeds  
  • Spammer feeds  
  • Commercial Threat intelligence providers  
  • Portscan / Web crawl data | • Search/Alert on your IP network or your supply chain’s network showing up on these lists.  
  • Periodic review of external internet facing assets |
| **Social Media and Dark Web** | • DarkWeb / DeepWeb Forums  
  • Social Media Sites  
  • Google Dorks | • Search/Alert on your brand or your supply chains’  
  • SIEM integrations |
| **Compromised Credentials** | • Paste sites  
  • DarkWeb / DeepWeb monitoring  
  • Google dorks  
  • Commercial Threat intelligence providers | • Search/Alert on your email domains or those of your supply chain  
  • Notify users  
  • Reset passwords as needed |
Conclusions

● Organizations must watch more than their industry vertical
● High Tech Suppliers such as Web and Domain Services, Firewall and Desktop Application vendors are increasingly targeted
● IoT used to pivot and maintain persistence.
● Vender Callback Tools (Performance/Monitoring) and Persistent VPN/Interconnected Networks are regularly abused
● Compromised Credentials may be used by third party contractors on your network

● Passive vendors audits
Contact

Jason Trost
• @jason_trost
• jason [dot] trost [AT] threatstream [dot] com
• https://github.com/jt6211

Nicholas Albright
• @nma_io
• nicholas [dot] albright [AT] threatstream [dot] com
• https://github.com/nma-io
Questions