

Inteligência de Ameaças Cibernéticas

Como aprimorar a detecção e resposta a ataques

7º Fórum Brasileiro de CSIRTs

Nichols Jasper

13/09/2018

Whoami

- Formado em Processamento de Dados pela FATEC-SP, pós-Graduado em Gestão da Segurança da Informação pelo IBTA-SP.
- Professor de segurança da informação na FATEC-SP.
- 10 anos em Consultoria de Segurança da Informação em diversas empresas, atualmente trabalho no *Blue Team* de uma instituição financeira.
- Fundador e consultor na [Spark Security](#).
- CISSP, CEH.

O que falaremos sobre Inteligência de Ameaças

- Conceitos
- Por que e Para que?
- Modelos
 - SANS Sliding Scale of Cybersecurity
 - Pyramid of Pain
 - Cyber Kill Chain
 - Diamond Model
- Caso Real - Detecção de Ameaças e Resposta a Incidentes



Conceitos

Inteligência - “todo o tipo de informações **sobre o inimigo e o seu país** - a base, em resumo, dos nossos planos e operações.”

Da Guerra - Carl Von Clausewitz – 1832

Uma boa inteligência deve ser acionável!

- **Completa** – suficiente para tomada de decisão
- **Acurada** – precisa para tomar uma boa decisão
- **Relevante** – relacionada a sua missão e objetivos
- **Oportuna** – entregue no tempo certo

Dragos - Industrial Control Threat Intelligence

Conceitos

Ameaça - “Fonte potencial de um **evento adverso**”

Computer Security Incident Handling Guide – NIST - SP 800-61 Rev. 2

Agente ou Ator de Ameaça - “São indivíduos, grupos ou organizações que realizam **ações maliciosas** contra determinado alvo. Podem ser caracterizados por suas motivações, capacidades, objetivos, nível de sofisticação, atividades passadas e recursos aos quais tem acesso.

STIX™ Version 2.0. Part 2: STIX Objects

Vetor de Ameaça - “A técnica ou o método utilizado por uma ameaça para comprometer a segurança do seu alvo, explorando suas vulnerabilidades”

SANS Glossary of Security Terms

Inteligência de Ameaças

*Threat intelligence is very simply **knowledge of the adversary (threats actors)**, it is generally analyzed information, meaning to some level of interpreted data and information relating to an entity that has the **intent, opportunity and capability** to do you **harm**.*

Robert M. Lee, CEO and founder of Dragos

Conhecimento

Contexto, Mecanismos,
Indicadores, Implicações,
Orientada a Ações

Adversário

Objetivos, comportamentos,
recursos, capacidades,
motivações, recursos

Por Quê?

- Das guerras antigas as modernas, conhecer bem seus inimigos é imperativo para o estabelecimento de estratégias eficientes.
- Para segurança da informação, a premissa também é válida.
- Sun Tzu, por volta de 500 anos A.C., escreveu a “A Arte da Guerra”, onde estabelecia:
 - “Conhece teu inimigo e conhece-te a ti mesmo; se tiveres cem combates a travar, cem vezes serás vitorioso.
 - Se ignoras teu inimigo e conheces a ti mesmo, tuas chances de perder e de ganhar serão idênticas.
 - Se ignoras ao mesmo tempo teu inimigo e a ti mesmo, só contarás teus combates por tuas derrotas.”



Para Quê?

1. Quais **tipos de atores** são uma **ameaça** a sua organização ou indústria
 - Capacidade, oportunidade e intenção.
2. Como estas ameaças **operam**?
3. Quais são as principais "**jóias da coroa**" que podem ser atacadas e abusadas em seu ambiente?
4. Qual o **risco** de sua empresa ser alvo destas ameaças?
 - Probabilidade X Impacto
5. Quais as melhores formas de vocês **prevenir, detectar e responder** a tais ameaças de maneira oportuna e proativa?

Sliding Scale of Cybersecurity



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

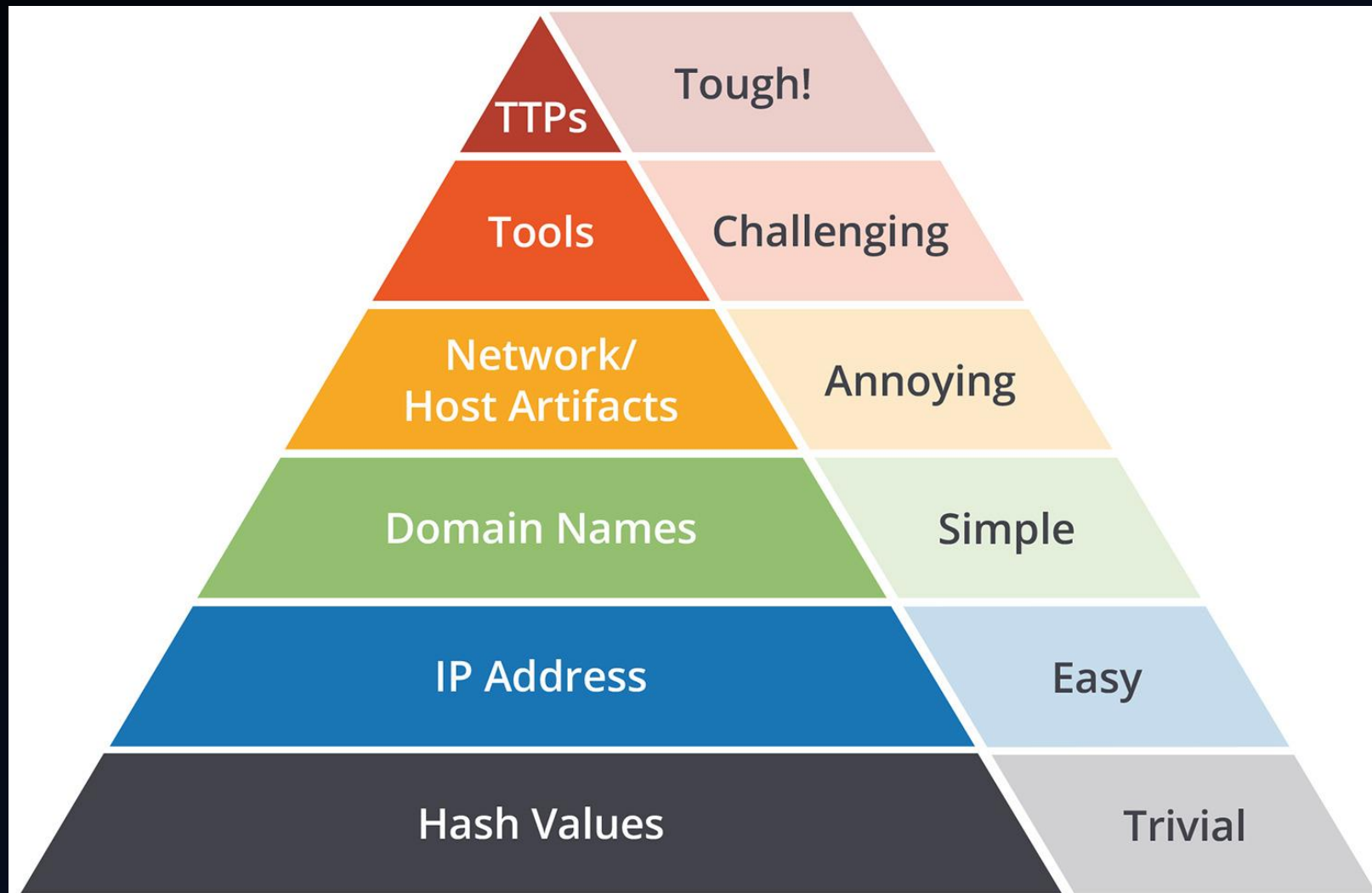
INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

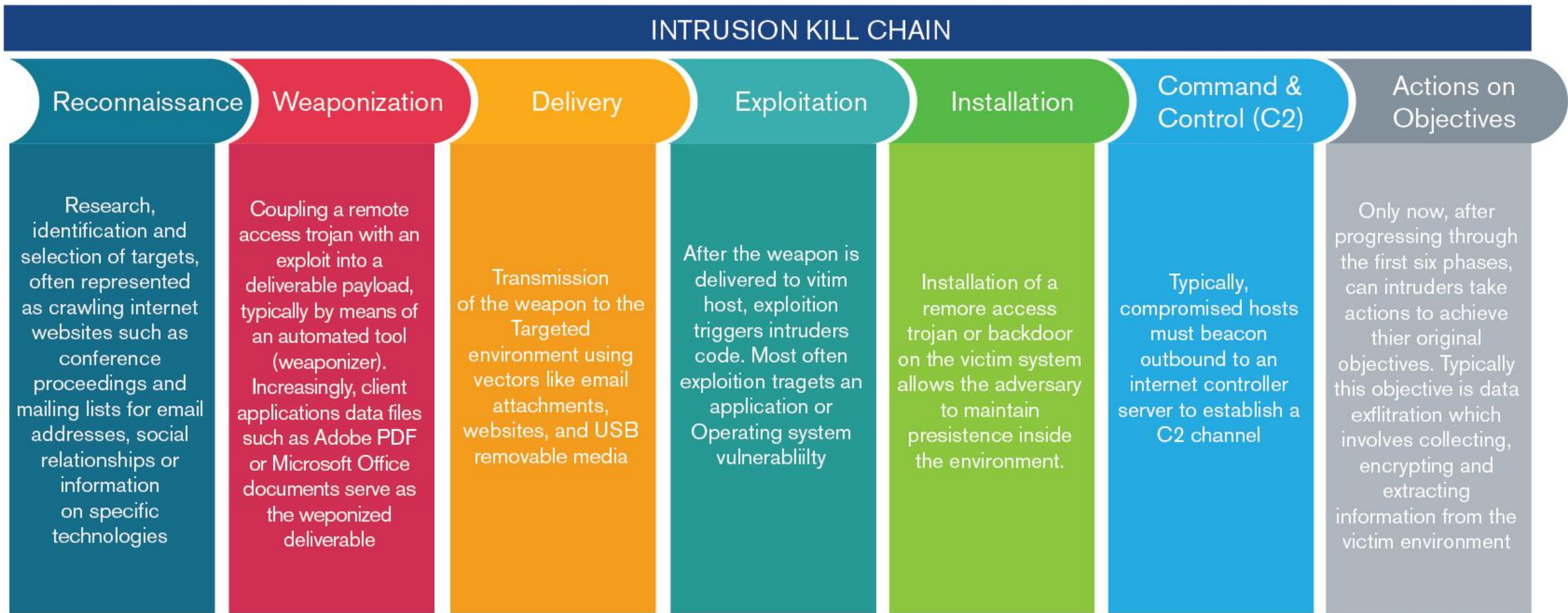
Legal countermeasures and self-defense actions against an adversary

Pyramid of Pain



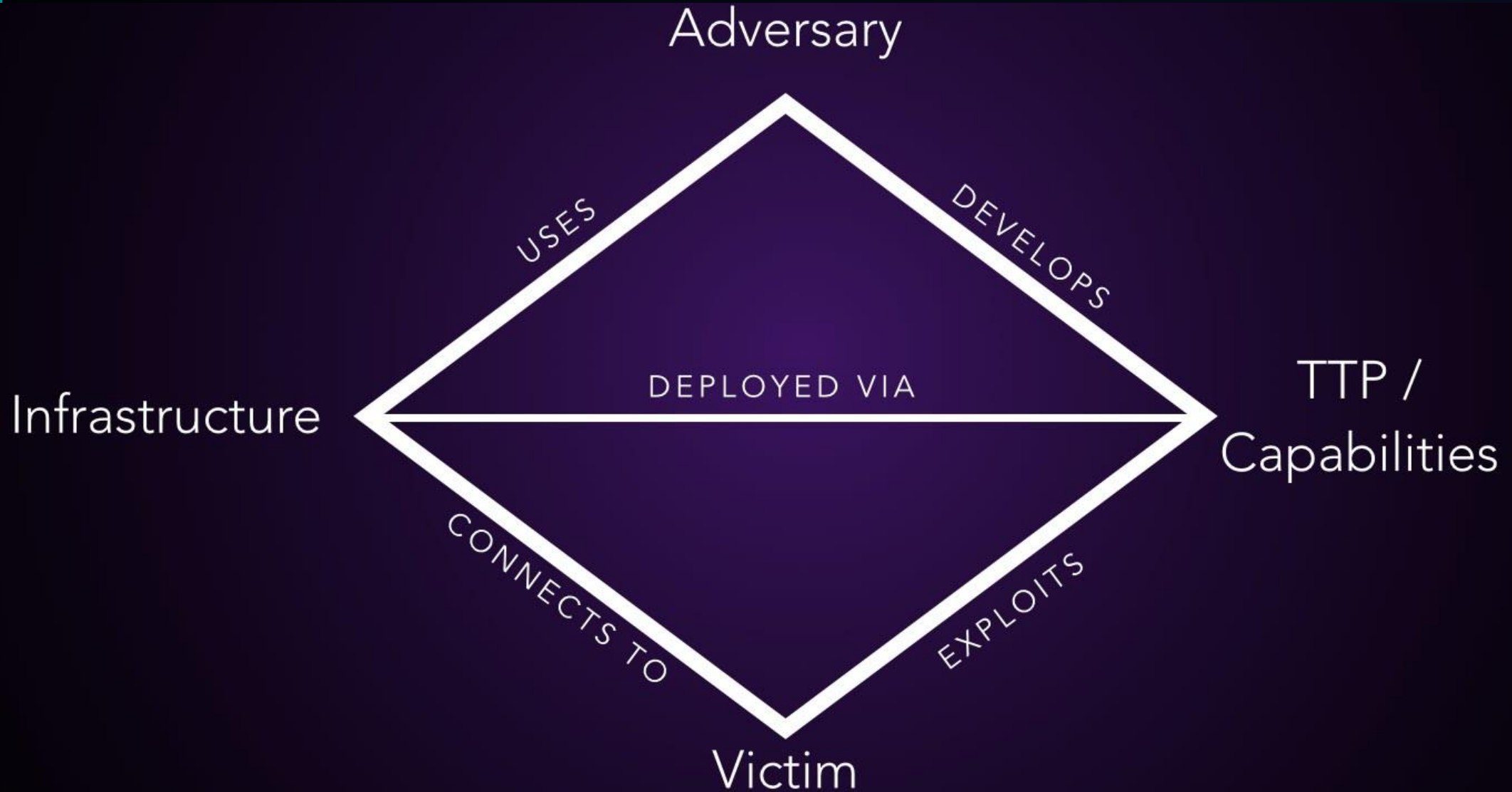
Source: David J. Bianco, personal blog

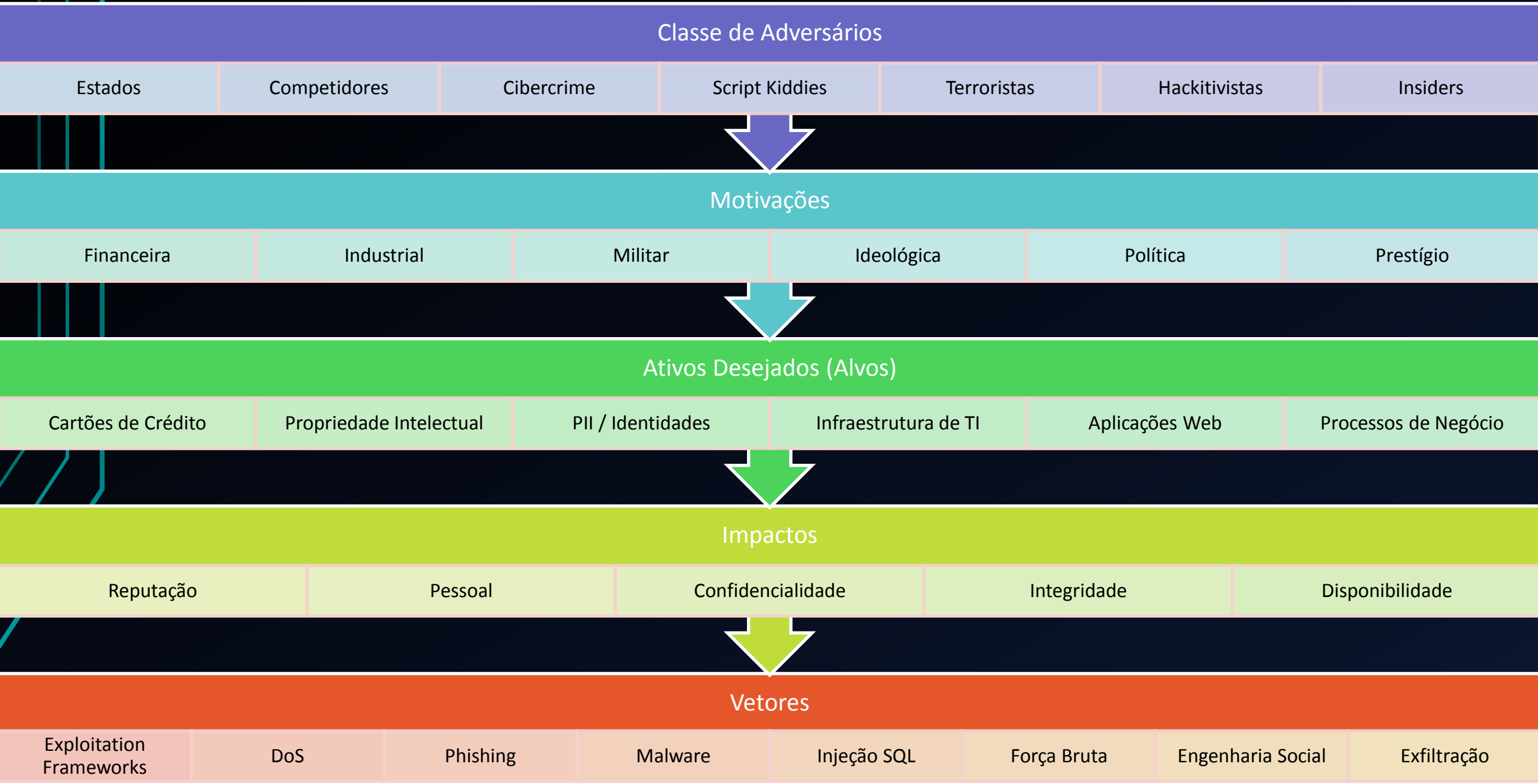
Cyber Kill Chain



Como o ator de ameaça opera, desde o reconhecimento até seu objetivo final?

Diamond Model for Intrusion Analysis





Classe de Adversários

Estados

Competidores

Cibercrime

Script Kiddies

Terroristas

Hacktivistas

Insiders

Motivações

Financeira

Industrial

Militar

Ideológica

Política

Prestígio

Ativos Desejados (Alvos)

Cartões de Crédito

Propriedade Intelectual

PII / Identidades

Infraestrutura de TI

Aplicações Web

Processos de Negócio

Impactos

Reputação

Pessoal

Confidencialidade

Integridade

Disponibilidade

Vetores

Exploitation Frameworks

DoS

Phishing

Malware

Injeção SQL

Força Bruta

Engenharia Social

Exfiltração



Perfilando Adversários – NSA 2013



APT & CyberCriminal Campaign Collection

APT & CyberCriminal Campaign Collection

This is a collection of APT and CyberCriminal campaigns. Please fire issue to me if any lost APT/Malware events/campaigns.

🔑 The password of malware samples could be 'virus' or 'infected'

Reference Resources

- [kbandla](#)
- [APTnotes](#)
- [Florian Roth - APT Groups](#)
- [Attack Wiki](#)
- [threat-INTel](#)
- [targetedthreats](#)
- 🍎 [Raw Threat Intelligence](#)
- [APT search](#)




2018









- Sep 04 - [\[Palo Alto Network\] OilRig Targets a Middle Eastern Government and Adds Evasion Techniques to OopsIE](#) | Local
- Aug 28 - [\[CheckPoint\] CeidPageLock: A Chinese RootKit](#) | Local
- Aug 23 - [\[Kaspersky\] Operation AppleJeu: Lazarus hits cryptocurrency exchange with fake installer and macOS malware](#) | Local
- Aug 21 - [\[ESET\] TURLA OUTLOOK BACKDOOR](#) | Local
- Aug 21 - [\[Trend Micro\] Supply Chain Attack Operation Red Signature Targets South Korean Organizations](#) | Local
- Aug 16 - [\[Recorded Future\] Chinese Cyberespionage Originating From Tsinghua University Infrastructure](#) | Local
- Aug 09 - [\[McAfee\] Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families](#) | Local
- Aug 02 - [\[Medium\] Goblin Panda against the Bears](#) | Local
- Jul 31 - [\[Palo Alto Network\] Bisonal Malware Used in Attacks Against Russia and South Korea](#) | Local
- Jul 31 - [\[Medium\] Malicious document targets Vietnamese officials](#) | Local
- Jul 16 - [\[Trend Micro\] New Andariel Reconnaissance Tactics Hint At Next Targets](#) | Local
- Jul 13 - [\[CSE\] Operation Roman Holiday – Hunting the Russian APT28 group](#) | Local

https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections

Aviso Importante!

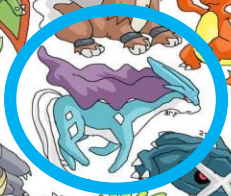
- Dragos
- Crowdstrike
- Nosso caso, Pokémon!

 <p>ALLANITE Since 2017</p>	 <p>CHRYSENE Since 2017</p>	 <p>XENOTIME Since 2014</p>
<p>MODE OF OPERATION Watering-hole and phishing leading to ICS recon and screenshot collection</p>	<p>MODE OF OPERATION IT compromise, information gathering and recon against industrial orgs</p>	<p>MODE OF OPERATION Focused on physical destruction and long-term persistence</p>
<p>CAPABILITIES Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSEXec</p>	<p>CAPABILITIES Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR</p>	<p>CAPABILITIES TRISIS, custom credential harvesting</p>
<p>VICTIMOLOGY Electric utilities, US & UK</p>	<p>VICTIMOLOGY Oil & Gas, Manufacturing, Europe, MENA, N. America</p>	<p>VICTIMOLOGY Oil & Gas, Middle East</p>
<p>LINKS Palmetto Fusion</p>	<p>LINKS OilRig, Greenbug</p>	<p>LINKS None</p>

Adversary	Category or Nation-State
 <p>BEAR</p>	Russian Federation
 <p>CHOLLIMA</p>	Democratic People's Republic of Korea (North Korea)
 <p>JACKAL</p>	Hactivist
 <p>KITTEN</p>	Iran
 <p>LEOPARD</p>	Pakistan
 <p>PANDA</p>	People's Republic of China
 <p>SPIDER</p>	eCrime
 <p>TIGER</p>	India



Suicune Group



Suicune Group



ADVERSARY

Grupo atuante desde 2016, com foco em instituições financeiras

Busca informações sensíveis na rede

Operava no fuso horário europeu

Campanhas duravam meses

Nmap / NSE
Cloud App Scan
(Qualys / Netsparker)
Webshell (LFI)
Injeção SQL
Mimikatz
Módulos Metasploit,
exploração de CVEs de
aplicações web
RDP sobre HTTPS
Força bruta em páginas
de administração



CAPABILITIES

Reconhecimento

Armamento

Entrega

Exploração

Instalação

C2

Ações



INFRASTRUCTURE

Proxy Reverso,
Múltiplos Proxies
VPS – Digital Ocean
– Cingapura /
Holanda / EUA
VPN / TOR



VICTIM

Instituições Bancárias
em vários países

Suicune Group - Ações

- Foram analisados os TTPs (táticas, técnicas e procedimentos) deste ator de ameaça para:
 - Determinar e priorizar a correção de vulnerabilidades exploradas no passado por este grupo.
 - Verificar junto as áreas de negócio a possibilidade de bloqueio de tráfego originado de alguns países, afinal, porque endereços de Cingapura acessam suas aplicações?
 - Aumentar a "paranoia" das equipes de monitoramento para alertas no horário comercial europeu, com especial atenção aos feriados locais.
 - Bloquear de tráfego oriundo de VPS/TOR/VPNs.
 - Criar alertas para monitorar atividades de reconhecimento e exploração.
 - Preparar ações de resposta para eventuais incidentes.



Conclusão

- Inteligência é sobre o inimigo, que pode já estar dentro da sua rede.
- Conhecer a si próprio é tão importante como conhecer seu inimigo.
- Inteligência de Ameaças pode (deve) apoiar toda atividade de segurança (operações, processos e estratégias).
- IA permite que o enfoque de segurança seja proativo e não reativo, apoiando na mitigação de riscos.
- “Contra ameaças, conhecimento é poder” – Fire Eye



Dúvidas?



Suicune Group

Referências

- SANS Sliding Scale of Cybersecurity - <https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240>
- The Pyramid of Pain - <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>
- Cyber Kill Chain - <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- The Diamond Model of Intrusion Analysis - Active Response - <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

Referências

- What Exactly Is Threat Intelligence? - <https://www.recordedfuture.com/podcast-episode-1/>
- Dragos Adversaries - <https://dragos.com/adversaries.html>
- Meet the Adversaries - <https://www.crowdstrike.com/blog/meet-the-adversaries/>
- The \$5 Vendor-Free Crash Course: Cyber Threat Intel - <https://tisiphone.net/2016/10/04/the-5-vendor-free-crash-course-cyber-threat-intel/>
- Tripwire - Threat Intelligence University
- Adversary ROI: Evaluating Security from the Threat Actor's Perspective - https://pt.slideshare.net/DavidEtue/adversary-roi-evaluating-security-from-the-threat-actors-perspective/12-Practical_Application_of_ROSI