Tempest

ACADEMY

Conference

2023

Cibersegurança em Tempos de Conflito

Navegando nas Fronteiras Digitais

Classificação da Informação: PÚBLICA
Autor da apresentação: <Josué Santos>

Tempest

:ACADEMY:

Conference

01 Sobre mim

02 Ameaças & Detecção

03 Elementos de Cibersegurança

04 Ações defensivas, preparem-se

Quem és tu, Josu?

Tempest
[ACADEMY]
Conference

+ 10 anos de experiência no mercado de Segurança da Informação, com formação em Gestão de Tecnologia e MBA em Cyber Security - Forensics, Ethical Hacking & DevSecOps;

Cursando Atualmente MBA em Gestão de Negócios: Cibersegurança e Proteção Digital;

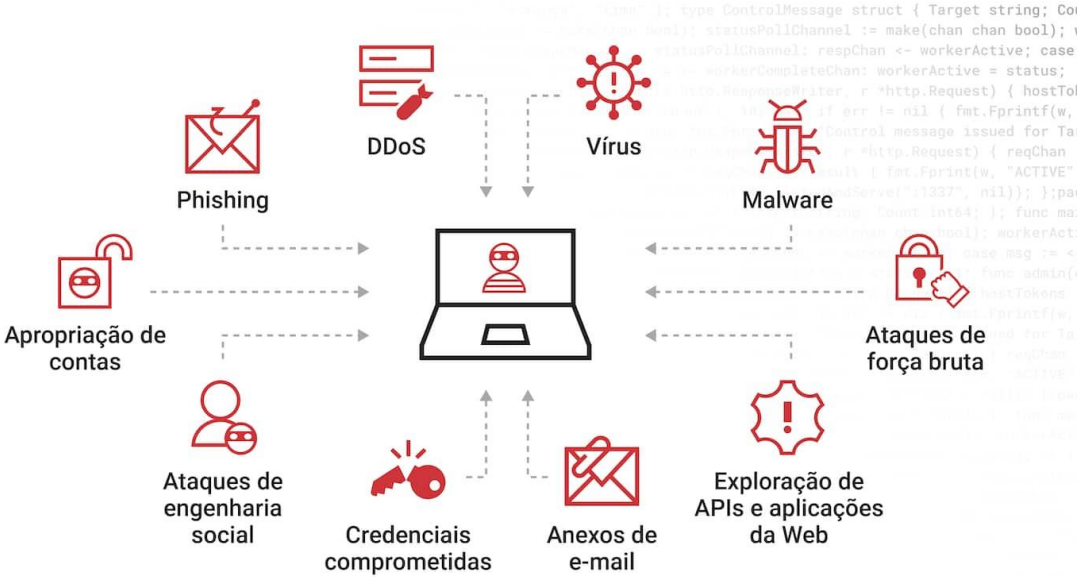
Certificações: ISO27001, ITIL, and IT Security, Ethical Hacking e Hacker Attack & Defense Cyber.

Participo nos programas sociais: Uuka, Projeto do Zero a Um e Projeto Somos UM.

Co-host e Partner no Podcast TecSec.

Eterno aprendiz.

A ameaça em CiberSegurança



Uma ameaça em segurança da informação refere-se a qualquer evento, processo ou entidade que tem o potencial de comprometer a confidencialidade, integridade ou disponibilidade dos dados ou sistemas de informação.

A detecção em CiberSegurança

Tempest
:ACADEMY:
Conference

A detecção em segurança da informação refere-se à identificação de atividades ou eventos suspeitos que podem indicar a presença de ameaças cibernéticas. O objetivo principal da detecção é identificar rapidamente incidentes de segurança para que a organização possa responder e mitigar potenciais danos.

A detecção em CiberSegurança

Tempest
:ACADEMY:
Conference

Detectar e mitigar ☺

Tempest

ACADEMY

Conference

Quais são os elementos ou tipos de cibersegurança?

- **Segurança da rede ou segurança da informação** defende contra ataques direcionados a vulnerabilidades e sistemas operacionais, arquitetura de rede, servidores, hosts, pontos de acesso sem fio e protocolos de rede.
- **Segurança na nuvem** protege dados, aplicações e infraestrutura residentes em nuvens públicas, privadas ou híbridas.
- **Segurança da IoT (Internet das coisas)** tem a tarefa de proteger milhares ou milhões de dispositivos que fazem parte de uma rede de IoT.
- **Segurança das aplicações** impede que invasores explorem as vulnerabilidades no software.
- **Gerenciamento de identidade e acesso** controla as permissões concedidas a indivíduos para acessar sistemas, aplicações e dados.
- **Segurança de pontos de extremidade** tem como foco a proteção de dispositivos conectados à Internet, como notebooks, servidores e celulares.
- **Soluções de segurança de dados** protegem dados confidenciais e ativos de informações em trânsito ou em repouso por meio de métodos como criptografia e backups de dados.

Tempest
[ACADEMY]
Conference

Voltando ao início!

Que conflitos são estes?

Crescente de Ataque vs Impacto

Tempest
[ACADEMY]
Conference

Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%

País é o 2º na América Latina com mais ataques cibernéticos em 2022

Brasil é um dos principais alvos de ataques cibernéticos no mundo

Em 2022, segundo relatório, o país só ficou atrás dos Estados Unidos em número de ciberataques

Por: Redação, 03/01/2023 às 11h09 - Atualizado em 03/01/2023 às 11h09

Brasil sofreu cerca de 1.600 ataques cibernéticos no primeiro semestre de 2023

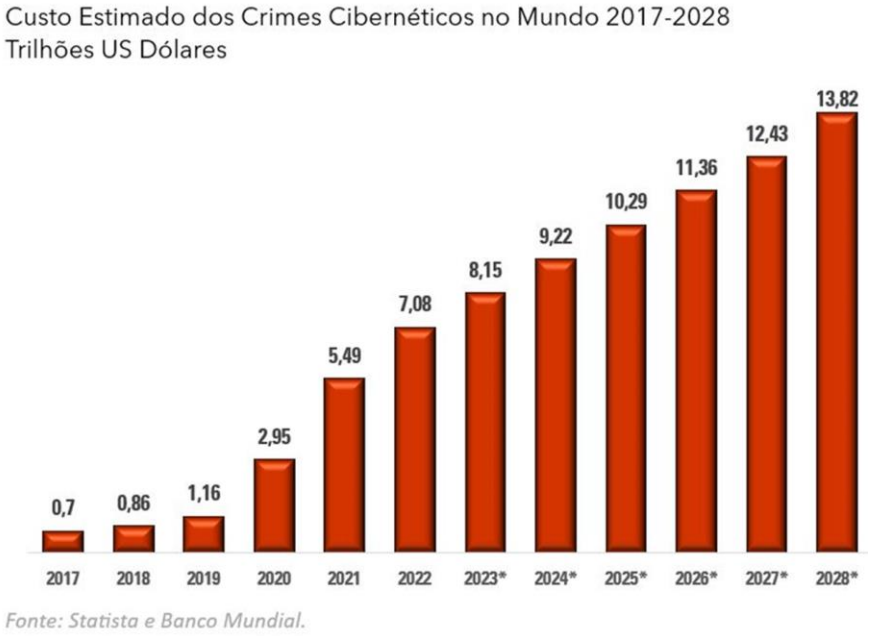
Relatório revela também aumento de 8% em ciberataques globais; e aponta ataques cibernéticos disruptivos que misturam técnicas e ferramentas novas e antigas

Brasil aparece em 2º em ranking de ataques cibernéticos; como se proteger

Regulação, compartilhamento de informações e os esforços de prevenção serão debatidos no Fides Rio 2023, o maior evento do mercado segurador nas Américas

Crescente de Ataque vs Impacto

Tempest
[ACADEMY]
Conference



Considerado os crimes cibernéticos efetivados entre 2017 e 2022, o custo acumulado chega a US$18,24 trilhões, superior ao PIB de acumulado, no mesmo período, pela Índia, a quinta maior economia do mundo

Guerra pelo no mundo, pode respingar no segmento cibernetico?

Tempest
[ACADEMY]
Conference

Tempest
ACADEMY
Conference

Tempest
[ACADEMY]
Conference

À medida que o conflito armado entre Israel e Palestina continua escalando, o número de grupos hacktivistas envolvidos a partir do ciberespaço tem aumentado. Esses grupos são classificados em grupos pró-Israel, grupos pró-Palestina e grupos que permanecem neutros.

Tempest [ACADEMY] Conference

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog Search

ATT&CK v14 has been released! Check out the blog post or release notes for more information.

GROUPS

- Overview
- admin@338
- Ajax Security Team
- ALLANITE
- Andariel
- Aoqin Dragon
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3

Home > Groups > admin@338

admin@338

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. [1]

ID: G0018

Contributors: Tatsuya Daitoku, Cyber Defense Institute, Inc.

Version: 1.2

Created: 31 May 2017

Last Modified: 18 March 2020

Version Permalink

Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: `net user >> %temp%\download net user /domain >> %temp%\download` [1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows	Following exploitation with LOWBALL malware, admin@338 actors created a file containing a list of commands to be executed on the compromised computer. [1]

Tempest

[ACADEMY]

Conference

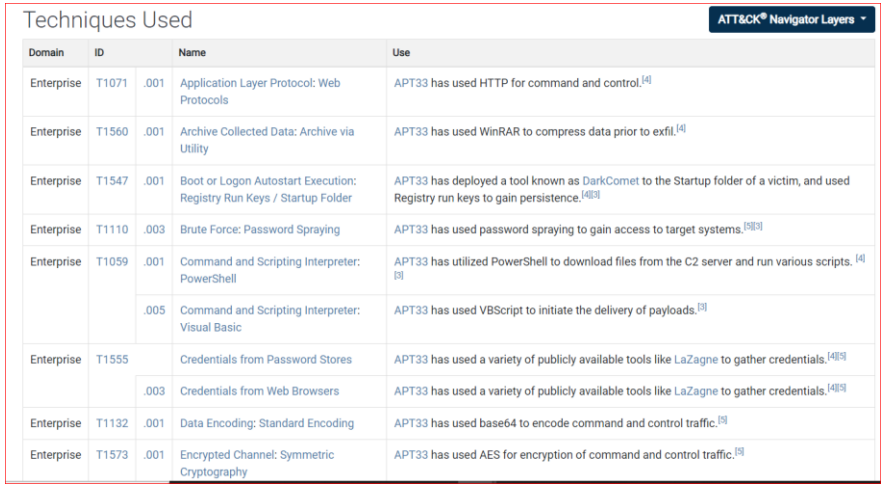
Ações defensivas

Tempest
[ACADEMY]
Conference

G0064	APT33	HÓLMIO, Elfin	O APT33 é um grupo suspeito de ameaça iraniana que realiza operações desde pelo menos 2013. O grupo tem como alvo organizações de vários setores nos Estados Unidos, Arábia Saudita e Coreia do Sul, com interesse particular nos setores da aviação e da energia.
G0049	Plataforma de petróleo	COBALT GYPSY, IRN2, APT34, Helix Kitten, Evasive Serpens	OilRig é um grupo suspeito de ameaça iraniana que tem como alvo vítimas do Médio Oriente e internacionais desde pelo menos 2014. O grupo tem como alvo uma variedade de sectores, incluindo financeiro, governamental, energético, químico e telecomunicações. Parece que o grupo realiza ataques à cadeia de abastecimento, aproveitando a relação de confiança entre organizações para atacar os seus alvos principais. A FireEye avalia que o grupo trabalha em nome do governo iraniano com base em detalhes de infraestrutura que contêm referências ao Irã, no uso da infraestrutura iraniana e na segmentação que se alinha aos interesses do Estado-nação.
G0087	APT39	[illegible] Saiipho	APT39 é um dos vários nomes para atividades de espionagem cibernética conduzidas pelo Ministério de Inteligência e Segurança iraniano (MOIS) por meio da empresa de fachada Rana Intelligence Computing desde pelo menos 2014. APT39 tem como alvo principal os setores de viagens, hospitalidade, acadêmico e telecomunicações no Irã e em toda a Ásia, África, Europa e América do Norte para rastrear indivíduos e entidades consideradas uma ameaça pelo MOIS.

Ações defensivas

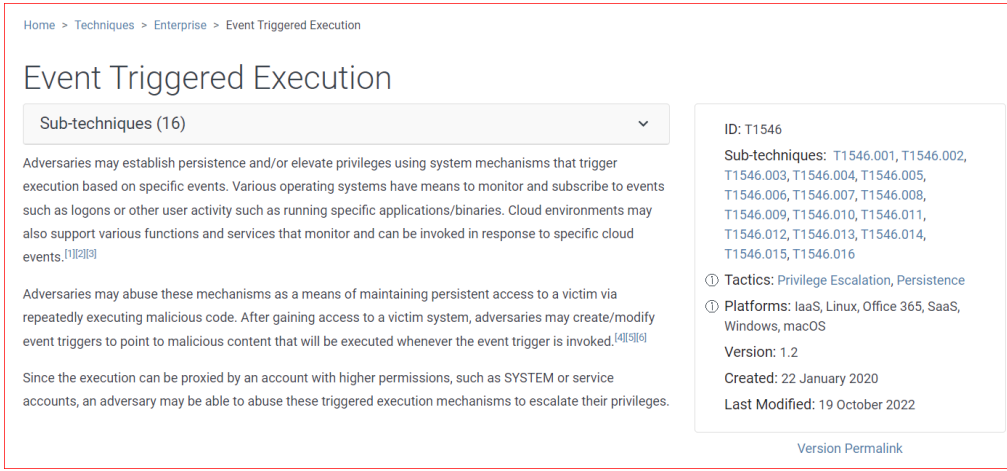
Tempest [ACADEMY] Conference



Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT33 has used HTTP for command and control.[4]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT33 has used WinRAR to compress data prior to exfil.[4]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT33 has deployed a tool known as DarkComet to the Startup folder of a victim, and used Registry run keys to gain persistence.[4][3]
Enterprise	T1110	.003	Brute Force: Password Spraying	APT33 has used password spraying to gain access to target systems.[5][3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT33 has utilized PowerShell to download files from the C2 server and run various scripts. [4] [3]
		.005	Command and Scripting Interpreter: Visual Basic	APT33 has used VBScript to initiate the delivery of payloads.[3]
Enterprise	T1555		Credentials from Password Stores	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
		.003	Credentials from Web Browsers	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	APT33 has used base64 to encode command and control traffic.[5]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	APT33 has used AES for encryption of command and control traffic.[5]



Home > Techniques > Enterprise > Event Triggered Execution

Event Triggered Execution

Sub-techniques (16)

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.[1][2][3]

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.[4][5][6]

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

ID: T1546

Sub-techniques: T1546.001, T1546.002, T1546.003, T1546.004, T1546.005, T1546.006, T1546.007, T1546.008, T1546.009, T1546.010, T1546.011, T1546.012, T1546.013, T1546.014, T1546.015, T1546.016

ⓘ Tactics: Privilege Escalation, Persistence

ⓘ Platforms: IaaS, Linux, Office 365, SaaS, Windows, macOS

Version: 1.2

Created: 22 January 2020

Last Modified: 19 October 2022

Version Permalink

Tempest
ACADEMY
Conference

Malware para Linux demonstra vínculo entre o grupo Lazarus e o ataque à cadeia de suprimentos

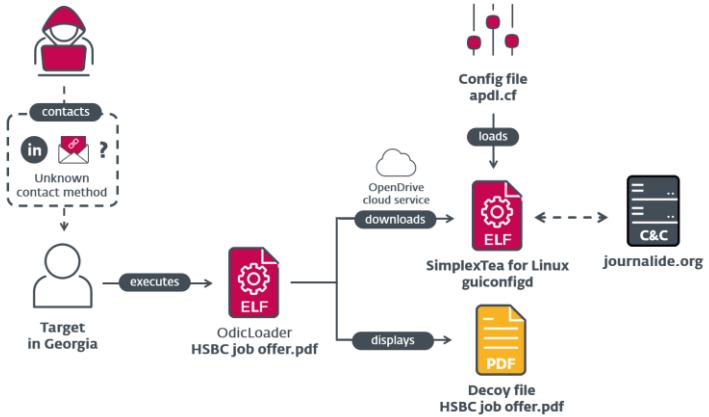
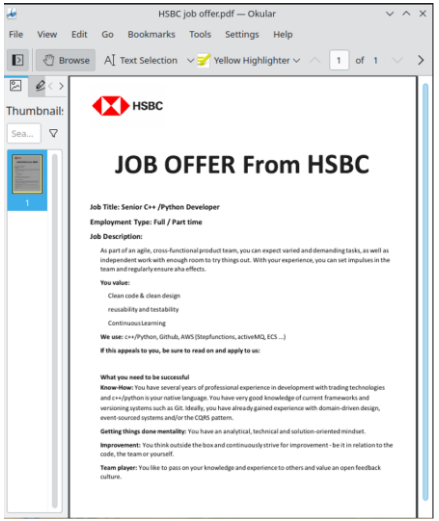


Ilustração da provável cadeia de comprometimento.



Isca usa o nome do HSBC na campanha da Operation DreamJob para Linux.

Tempest

ACADEMY

Conference

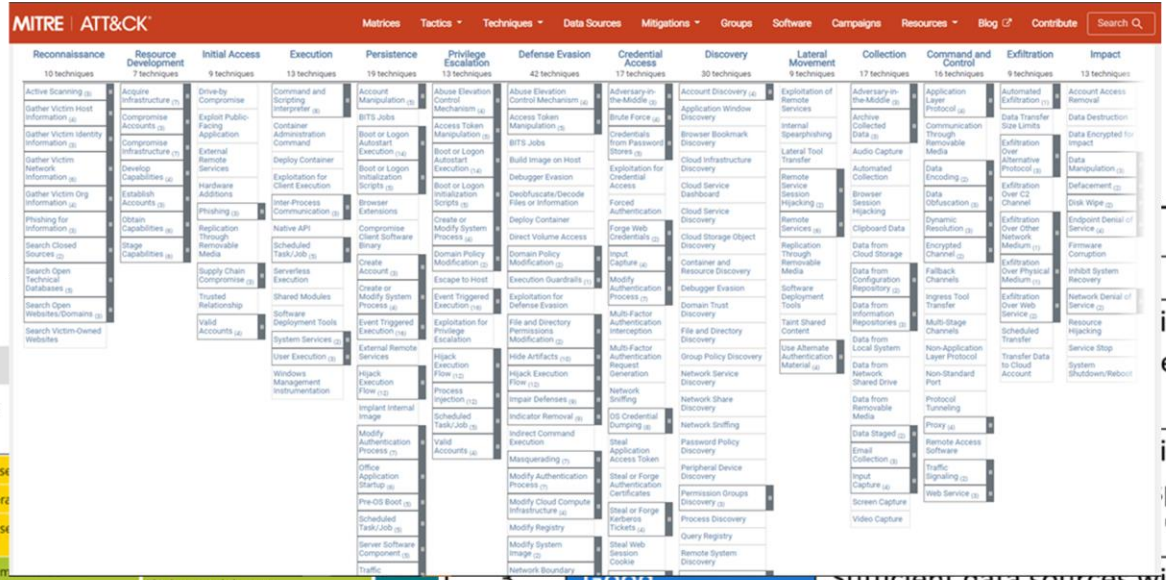
Malware para Linux demonstra vínculo entre o grupo Lazarus e o ataque à cadeia de suprimentos

O ataque à cadeia de suprimentos da 3CX atraiu muita atenção da comunidade de segurança desde sua divulgação em 29 de março. O software comprometido, implantado em várias infraestruturas de TI, permite o download e a execução de qualquer tipo de payload, portanto, o impacto de um ataque desse tipo pode ser devastador. Infelizmente, nenhum fornecedor de software está imune a ser comprometido e a distribuir inadvertidamente versões trojanizadas de seus aplicativos.

Fonte: welivesecurity

Preparem-se...

Tempest
[ACADEMY]
Conference



RE&CT Enterprise Matrix

Preparation	Identification	
103 items	63 items	
Practice	List victims of s	
Take trainings	List host vulner	
Raise personnel awareness	Put compromise monitoring	
Make personnel report suspicious activity	List hosts comm internal domain	Block internal domain
Set up relevant data collection	List hosts communicated with internal IP	Block external URL
Set up a centralized long-term log storage		Block internal URL
Develop communication map	List hosts communicated with internal URL	Block port external communication
Make sure there are backups	Analyse domain name	Block port internal communication
Get network architecture map	Analyse IP	Block user external communication
Get access control matrix	Analyse uri	Block user internal communication
Develop assets knowledge base	List hosts communicated by port	Block data transferring by content pattern
Check analysis toolset	List hosts connected to VPN	Block domain on email
Access vulnerability management system logs	List hosts connected to intranet	Block sender on email
	List data transferred	

		ith sufficient quality available
		ect of the technique's
		ith sufficient quality available
		pects of the technique's
		"1/Minimal".
3	Good	Sufficient data sources with sufficient quality available to be able to see almost all known aspects of the technique's procedures.
4	Excellent	All data sources and required data quality necessary to be able to see all known aspects of the technique's procedures are available.

Remove re
Remove se
Revoke au
Remove u

Enable disabled service
Unlock locked user account

Tempest
[ACADEMY]
Conference

...para surpreender

Obrigado

Tempest
ACADEMY
Conference