



Tempest

ACADEMY

Conference
2023

Cibersegurança em Tempos de Conflito

Navegando nas Fronteiras
Digitais





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 **detecção** em CiberSegurança

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 😊



Quais são os elementos ou tipos de cibersegurança?

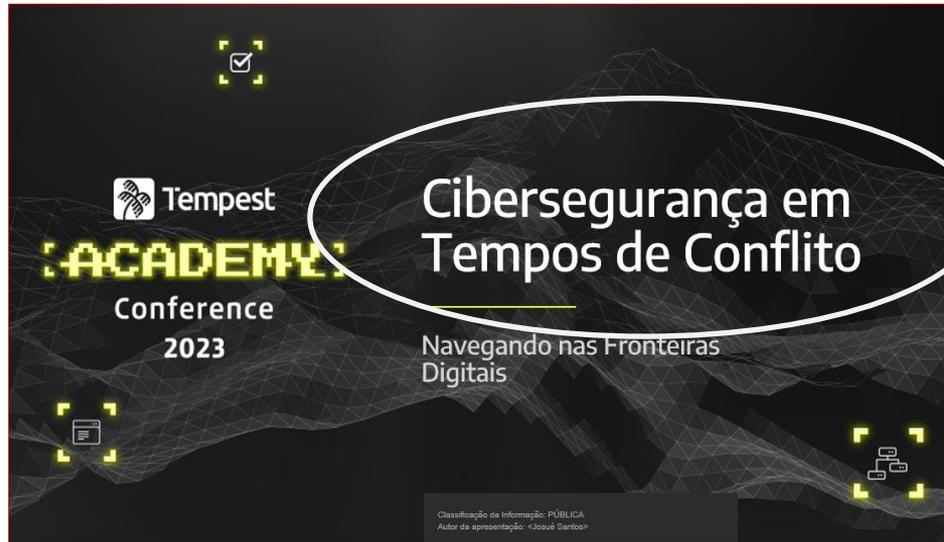
- **Segurança da rede ou segurança da informação** defende contra ataques direcionados a vulnerabilidades e sistemas operacionais, arquitetura de rede, servidores, hosts, pontos de acesso sem fio e protocolos de rede.
- **Segurança na nuvem** protege dados, aplicações e infraestrutura residentes em nuvens 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

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

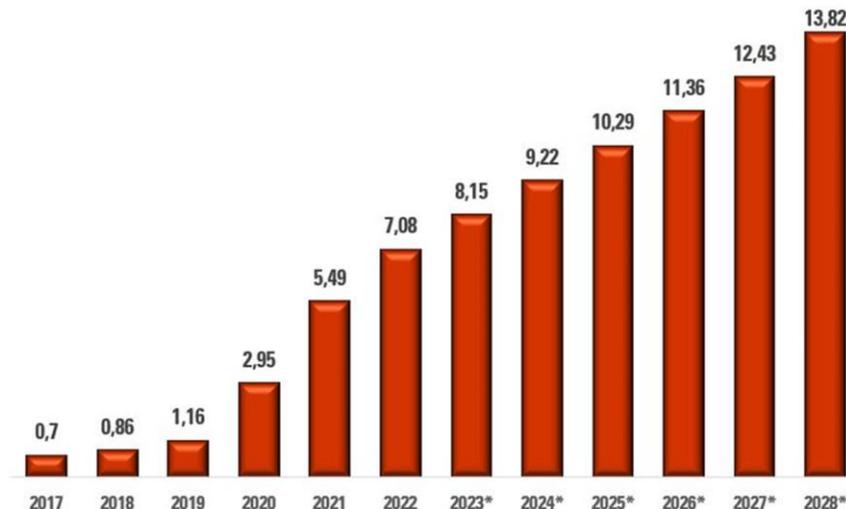
Relatório revela também aumento de 8% em ciberataques globais; e aponta ataques cibernéticos disruptivos que misturam técnicas e ferramentas novas e antigas

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

Custo Estimado dos Crimes Cibernéticos no Mundo 2017-2028
Trilhões US Dólares



Fonte: Statista e Banco Mundial.

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 mundo, pode respingar no segmento cibernético?

Tempest

ACADEMY

Conference



SiM!

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.



[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.

Home > Groups > admin@338

GROUPS

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

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](#)

[ATT&CK® Navigator Layers ▾](#)

Techniques Used

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: <code>net user >> %temp%\download net user /domain >> %temp%\download^[1]</code>
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]

IRoX Team
173 subscribers

[Pinned Message #4](#)
Photo, Good Morning Indian Ci...

Today

Cyber Attack Warning - IRoX Team

We always stand by our Palestinian Muslim brothers. We have declared cyber war against Israel as well as those who support Israel.

The scheduled cyber attacks are as follows:

1. Date: 20th October 2023
Targeted Countries - Brazil, Canada, Poland, Spain
2. Date: 25th October 2023
Targeted Country - India, United Kingdom, Australia
3. Date: 30th October 2023
Targeted Country - France, Norway, Austria, Germany

We will completely destroy the cyberspace of those who support Israeli Jews.
We are not organization... We are Community with Unity!
Our Decision is not depends on One Group! Expect us!
We are IRoX COMMUNITY

[Join Us » @IRoX_Team](#)

❤️ 11 🔥 3 🍷 1 🙌 1

532 👁️ 04:20 AM

13 Comments



Tempest

[ACADEMY]

Conference



Ações defensivas

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 contém referências ao Irã, no uso da infraestrutura iraniana e na segmentação que se alinha aos interesses do Estado-nação.
G0087	APT39	Iran - Jafinho	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

Techniques Used

[ATT&K® 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. ^{[3][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	.001 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. ^[3]
Enterprise	T1573	.001 Encrypted Channel: Symmetric Cryptography	APT33 has used AES for encryption of command and control traffic. ^[3]

[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**① Tactics:** Privilege Escalation, Persistence**① Platforms:** IaaS, Linux, Office 365, SaaS, Windows, macOS**Version:** 1.2**Created:** 22 January 2020**Last Modified:** 19 October 2022[Version Permalink](#)

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

Tempest
ACADEMY
Conference

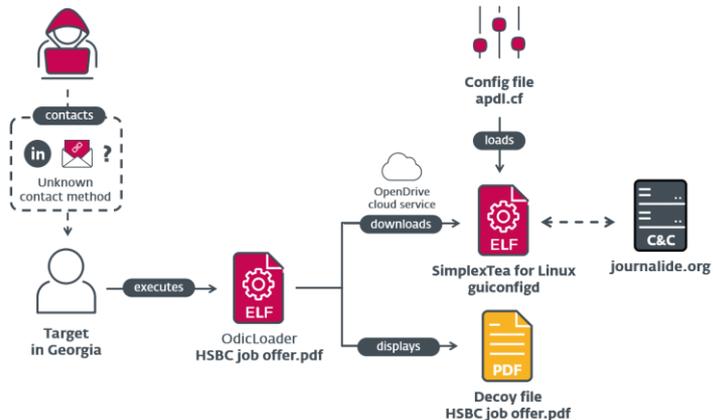
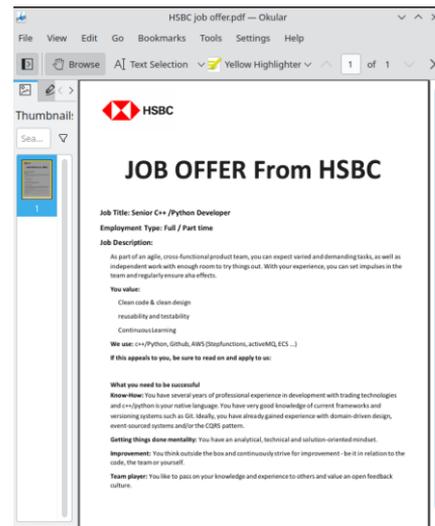


Ilustração da provável cadeia de comprometimento.



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

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](#)

 Tempest

ACADEMY

Conference

Preparation-se...



ACADEMY

Conference

MITRE ATT&CK													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	14 techniques	9 techniques	13 techniques
Active Scouting (2)	Acquire Infrastructure (2)	Drive-by Compromise (2)	Command and Scripting Interference (2)	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services (2)	Adversary in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal (2)
Garther Victim Host Information (2)	Exploit Public-Facing Application (2)	External Remote Services (2)	Container Administration Command (2)	Boot or Logon Autostart Execution (2)	Access Token Manipulation (2)	Access Token Manipulation (2)	Stuxnet (2)	Browser Bookmark Discovery (2)	Internal Spearphishing (2)	Archive Collected Data (2)	Communication Through Removable Media (2)	Data Transfer Size Limits (2)	Data Destruction (2)
Garther Victim Identity Information (2)	External Remote Services (2)	Hardware Additions (2)	Deploy Container (2)	Boot or Logon Autostart Execution (2)	Build Image on Host (2)	Build Image on Host (2)	Credentials from Password Stores (2)	Cloud Infrastructure Discovery (2)	Debugger Evasion (2)	Audio Capture (2)	Data Encoding (2)	Data Manipulation (2)	Data Encrypted for Impact (2)
Garther Victim Network Information (2)	Establish Accounts (2)	Phishing (2)	Exploitation for Client Execution (2)	Boot or Logon Initialization Scripts (2)	Debugger Evasion (2)	Debugger Evasion (2)	Forge Web Credentials (2)	Cloud Service Dashboard (2)	Remote Session Hijacking (2)	Automated Collection (2)	Data Obfuscation (2)	Defacement (2)	Data Manipulation (2)
Search Closed Sources (2)	Search Open Technical Databases (2)	Search Open Websites/Domain (2)	Search Victim-Owned Websites (2)	Native API (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (2)	Container and Resource Discovery (2)	Remote Service (2)	Clipboard Data (2)	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (2)	Endpoint Denial of Service (2)
Search Open Websites/Domain (2)	Search Victim-Owned Websites (2)	Supply Chain Compromise (2)	Trusted Relationship (2)	Scheduled Task/Job (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Mobile Authentication (2)	Software Deployment Tools (2)	Replication Through Removable Media (2)	Data from Cloud Storage (2)	Fallback Channels (2)	Exfiltration Over Physical Medium (2)	Firmware Corruption (2)
Search Victim-Owned Websites (2)	Windows Management Instrumentation (2)	Valid Accounts (2)	Software Deployment Tools (2)	Event Triggered Execution (2)	Event Triggered Execution (2)	Event Triggered Execution (2)	Multi-Factor Authentication Interception (2)	Debugger Evasion (2)	Software Deployment Tools (2)	Data from Information Repositories (2)	Ingress Tool Transfer (2)	Exfiltration Over Web Service (2)	Network Denial of Service (2)
			System Services (2)	Event Triggered Execution (2)	Exploitation for Privilege Escalation (2)	Exploitation for Privilege Escalation (2)	Multi-Factor Authentication Request Generation (2)	Domain Trust Discovery (2)	Tarnt Shared Content (2)	Data from Network Shared Drive (2)	Non-Application Layer Protocol (2)	Scheduled Transfer (2)	Service Stop (2)
			User Execution (2)	External Remote Services (2)	Hide Artifacts (2)	Hide Artifacts (2)	Network Service Discovery (2)	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (2)	Data from Local System (2)	Non-Standard Port (2)	Transfer Data to Cloud Account (2)	System Shutdown/Reboot (2)
			Windows Management Instrumentation (2)	Implant Internal Image (2)	Process Injection (2)	Process Injection (2)	Network Sniffing (2)	File and Directory Permissions Modification (2)	Group Policy Discovery (2)	Data from Network (2)	Protocol Tunneling (2)		
				Scheduled Task/Job (2)	Indicator Removal (2)	Indicator Removal (2)	OS Credential Dumping (2)	Multi-Factor Authentication Request Generation (2)	Network Service Discovery (2)	Impair Data from Removable Media (2)	Protocol Tunneling (2)		
				Modify Authentication Process (2)	Indirect Command Execution (2)	Indirect Command Execution (2)	Network Sniffing (2)	Stall or Forge Authentication Certificates (2)	Peripheral Device Discovery (2)	Network Sniffing (2)	Protocol Tunneling (2)		
				Maneuvering (2)	Modify Authentication Process (2)	Modify Authentication Process (2)	Stall or Forge Authentication Certificates (2)	Stall or Forge Authentication Certificates (2)	Permission Groups Discovery (2)	Network Sniffing (2)	Protocol Tunneling (2)		
				Pre-OS Boot (2)	Modify Cloud Computation Infrastructure (2)	Modify Cloud Computation Infrastructure (2)	Stall or Forge Authentication Certificates (2)	Stall or Forge Authentication Certificates (2)	Process Discovery (2)	Network Sniffing (2)	Protocol Tunneling (2)		
				Scheduled Task/Job (2)	Modify Registry (2)	Modify Registry (2)	Stall or Forge Authentication Certificates (2)	Stall or Forge Authentication Certificates (2)	Query Registry (2)	Network Sniffing (2)	Protocol Tunneling (2)		
				Server Software Component (2)	Modify System Image (2)	Modify System Image (2)	Stall or Forge Authentication Certificates (2)	Stall or Forge Authentication Certificates (2)	Remote System Discovery (2)	Network Sniffing (2)	Protocol Tunneling (2)		
				Traffic (2)	Network Boundary (2)	Network Boundary (2)	Stall or Forge Authentication Certificates (2)	Stall or Forge Authentication Certificates (2)	Remote System Discovery (2)	Network Sniffing (2)	Protocol Tunneling (2)		

RE&CT Enterprise Matrix x +

Preparation 103 items Identification 63 items

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

5 Good

4 Excellent

Enable disabled service

Unlock locked user account

ith sufficient quality available
ect of the technique's

ith sufficient quality available
pects of the technique's
"1/Minimal".

sufficient data sources with sufficient quality available
to be able to see almost all known aspects of the
technique's procedures.

All data sources and required data quality necessary to
be able to see all known aspects of the technique's
procedures are available.

...para surpreender

 Tempest
:ACADEMY:
Conference





Obrigado



[ACADEMY]
Conference



Tempest



ACADEMY

Conference

2023

