Cybercrime & Cyberwar

IT-SA 2022

WITH secure

Rüdiger

WITH secure

Rüdiger Trost

WITH secure

Rüdiger
Trost
Freue

WITH secure

Rüdiger
Trost
Freue
Mich

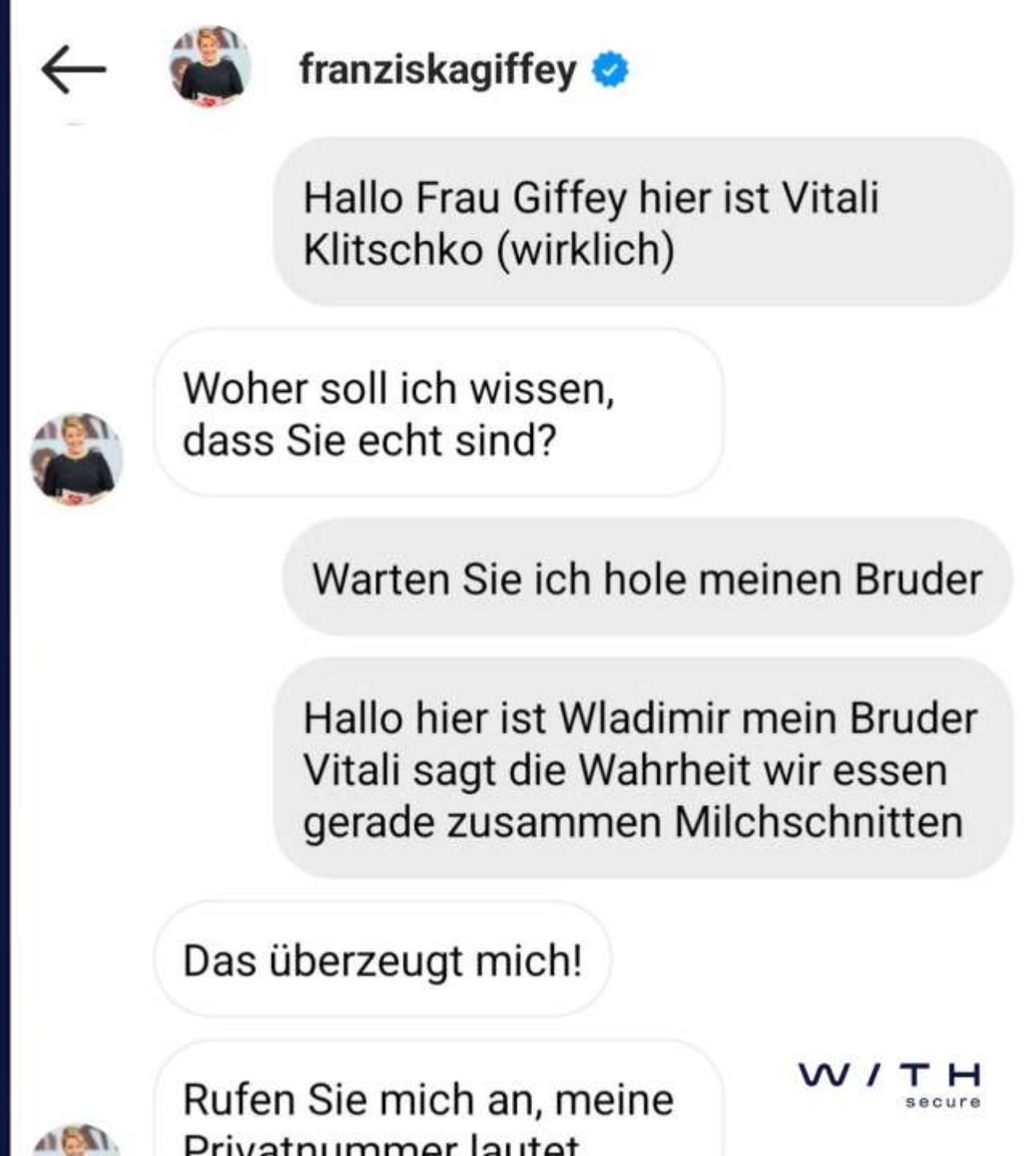
WITH secure

R
T
F
M

W/TH
secure

Cybercrime & Cyberwar

IT-SA 2022



WITH secure

Cybercrime & Cyberwar

2013

Rüdiger Trost

F-Secure.

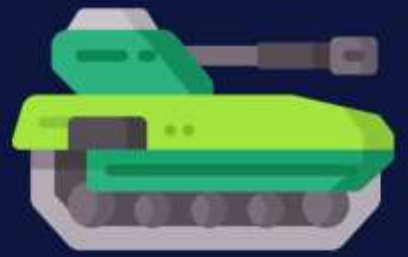
2014
CYBERCRIME
AND
CYBERWAR
F-Secure.

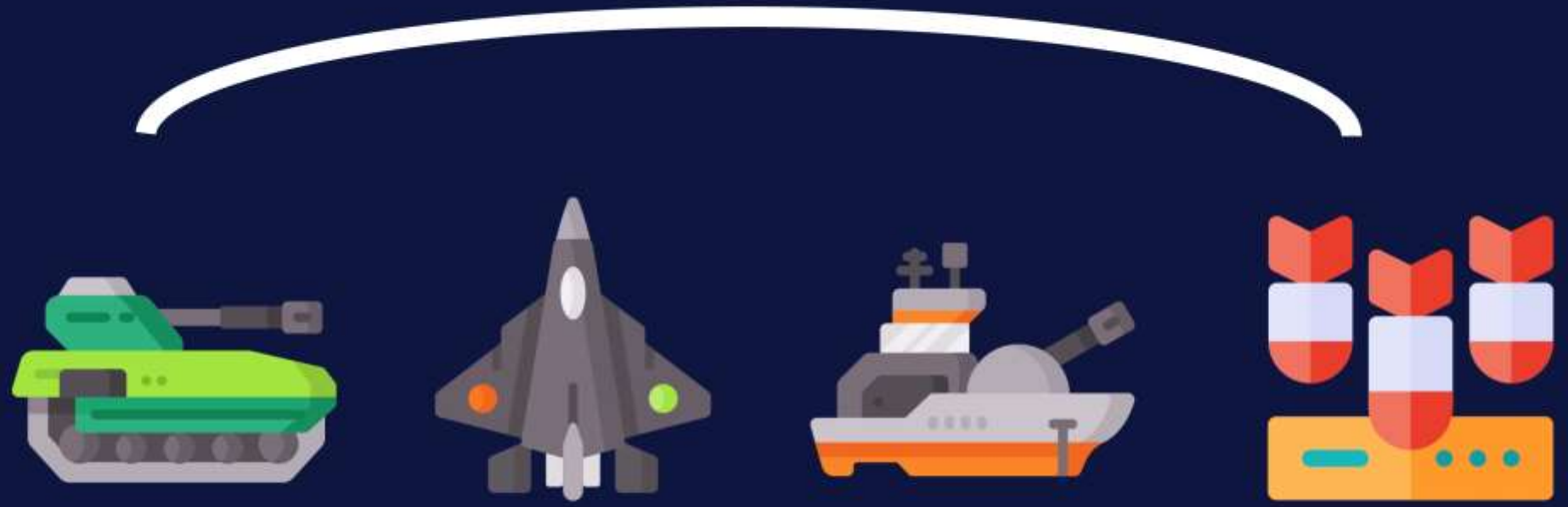
2015

CYBERCRIME AND CYBERWAR

F-Secure

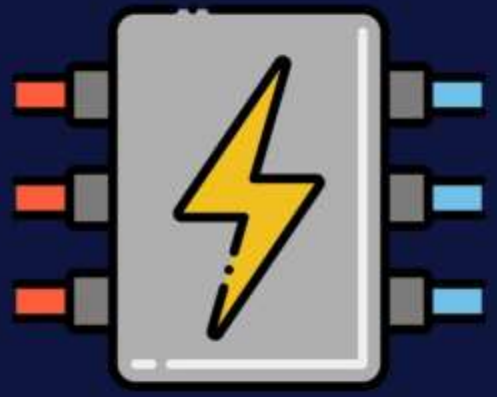
CYBERCRIME AND CYBERWAR





HermeticWiper

Jeep
AT 9570 E



1. Effektiv

1. Effektiv

2. Bezahlbar

1. Effektiv

2. Bezahlbar

3. Abstreitbar

1. Effektiv

2. Bezahlbar

USP

3. Abstreitbar

STUXNET

WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Zufälliger Artikel

Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe
Letzte Änderungen
Kontakt
Spenden

Werkzeuge
Links auf diese Seite
Änderungen an verlinkten Seiten
Spezialseiten
Permanenter Link
Seiteninformationen
Artikel zitieren
Wikidata-Datenobjekt

Drucken/exportieren
Als PDF herunterladen
Druckversion

In anderen Projekten
Commons

In anderen Sprachen
English
Español
Français
Italiano
Nederlands
Polski
Русский
Türkçe
中文
27 weitere
Links bearbeiten

Stuxnet

Stuxnet ist ein Computerwurm, der im Juni 2010 entdeckt und zuerst unter dem Namen **RootkitTmphider** beschrieben wurde.[T 1] Das Schadprogramm wurde speziell entwickelt zum Angriff auf ein System zur Überwachung und Steuerung (SCADA-System) des Herstellers Siemens – die Simatic S7. Dabei wurde in die Steuerung von Frequenzumrichtern der Hersteller *Vacon* aus Finnland und *Fararo Paya* in Teheran eingegriffen. Frequenzumrichter dienen beispielsweise dazu, die Geschwindigkeit von Motoren zu steuern.

Solche Steuerungen werden vielfach eingesetzt, etwa in Industrieanlagen wie Wasserwerken, Klimatechnik oder Pipelines.[T 2]

Da bis Ende September 2010 der Iran den größten Anteil der infizierten Computer besaß[T 3] und es zu außergewöhnlichen Störungen im iranischen Atomprogramm kam, lag es nah, dass Stuxnet hauptsächlich entstand, um die Leittechnik der Urananreicherungsanlage in Natanz[1] oder des Kernkraftwerks Buschehr[2] zu stören.

Die hochversierte Programmierer-Gruppe und Auftraggeber sind unbekannt.[T 4] Jedoch leitete das US-Justizministerium im Jahr 2013 Ermittlungen gegen Stuxnet-Projektleiter General James E. Cartwright ein.[3] Die Behörde vermutete, dass dieser im Jahr 2010 Details zu Stuxnet an die New York Times weitergab, was mutmaßlich zur Enttarnung des 50 Millionen Dollar teuren Sabotageprogramms führte.[3] Eine Anklage gegen Cartwright in der Sache selbst erfolgte nicht. Allerdings wurde er wegen einer Falschaussage bei den Ermittlungen angeklagt, jedoch 2017 noch vor einem Urteil von Präsident Barack Obama begnadigt.

Stuxnet	
Name	Stuxnet
Aliase	RootkitTmphider
Bekannt seit	entdeckt am 17. Juni 2010
Herkunft	USA, Israel (unbestätigt)
Typ	Netzwerkwurm
Weitere Klassen	Wechseldatenträger-Wurm Rootkit
Dateigröße	ca. 500 KByte
Speicherresident	ja
Verbreitung	mehrere Windows Exploits
System	MS Windows
Programmiersprache	C, C++ und andere
Info	Professionelle Sabotagesoftware für Cyberattacken gegen iranische Atomanlagen, vermutlich im Auftrag von Pentagon und Mossad.

Inhaltsverzeichnis [Verbergen]

1 Eigenschaften und Besonderheiten
2 Infektionsweg
2.1 Betriebssystem-Ebene
2.2 WinCC-Software
2.3 Eingriff in die speicherprogrammierbare Steuerung
2.4 Aktualisierungen und Abruf von Daten
3 Verbreitung
4 Vermutungen über die Urheber und Ziele
4.1 Experten und Ingenieure
4.2 Zum Auftraggeber Israel
4.3 Zum Auftraggeber Vereinigte Staaten
4.4 Zu einer Gemeinschaftsarbeit mehrerer Staaten
4.5 Ziele
5 Nachfolger Duqu
6 Trivia
7 Literatur
8 Weblinks
9 Anmerkungen
9.1 Technische Beschreibungen
9.2 Einzelnachweise

Eigenschaften und Besonderheiten [Bearbeiten | Quelltext bearbeiten]

Stuxnet gilt aufgrund seiner Komplexität und des Ziels, Steuerungssysteme von Industrieanlagen zu sabotieren, als bisher einzigartig. Die öffentlich verfügbaren Erkenntnisse basieren auf den Aussagen von IT-Fachleuten, die ausführbare Dateien der Schadsoftware analysierten. Die Beurteilungen basieren teilweise auf Interpretationen, da der Quelltext der Urheber nicht veröffentlicht ist.

Aufgrund der Komplexität von Stuxnet wird ein für eine Schadsoftware außerordentlich hoher Entwicklungsaufwand vermutet. Der Zeitaufwand wird bei einer vorhandenen Testumgebung für Hard- und Software auf mindestens sechs Monate, der Personalaufwand auf mindestens fünf bis zehn Hauptentwickler sowie zusätzliches Personal für Qualitätssicherung und Management geschätzt. Neben dem Fachwissen für die Entwicklung der Software mussten Kenntnisse über unbekannte Sicherheitslücken und Zugang zu geheimen Signaturen zweier Unternehmen vorhanden sein. Die Unternehmen mit den frühesten Anzeichen einer Stuxnet-Infektion waren Zulieferer. Daher wurde das Schadprogramm indirekt, über das Partnernetzwerk eingeschleust.[4]

oder Pipelines.[T 2]

ergewöhnlichen Störungen im iranischen Atomprogramm kam, lag es nah, dass Stuxnet
rks Buschehr[2] zu stören.

zministerium im Jahr 2013 Ermittlungen gegen Stuxnet-Projektleiter General James E. Cartwright
b, was mutmaßlich zur Enttarnung des 50 Millionen Dollar teuren Sabotageprogramms führte.[3]
ssage bei den Ermittlungen angeklagt, jedoch 2017 noch vor einem Urteil von Präsident Barack

Aliase	RootkitTmphider
Bekannt seit	entdeckt am 17. Juni 2010
Herkunft	USA, Israel (unbestätigt)
Typ	Netzwerkwurm
Weitere Klassen	Wechseldatenträger-Wurm Rootkit
Dateigröße	ca. 500 KByte
Speicherresident	ja
Verbreitung	mehrere Windows Exploits
System	MS Windows
Programmiersprache	C, C++ und andere
Info	Professionelle Sabotagesoftwar für Cyberattacken gegen iranisc Atomanlagen, vermutlich im Auf von Pentagon und Mossad.

t zum Angriff auf ein System
nnland und *Fararo Paya* in

nah, dass Stuxnet

eneral James E. Cartwright
otageprogramms führte.[3]
rteil von Präsident Barack

Stuxnet	
Name	Stuxnet
Aliase	RootkitTmphider
Bekannt seit	entdeckt am 17. Juni 2010
Herkunft	USA, Israel (unbestätigt)
Typ	Netzwerkwurm
Weitere Klassen	Wechseldatenträger-Wurm Rootkit
Dateigröße	ca. 500 KByte
Speicherresident	ja

Stuxnet	
	Stuxnet
	RootkitTmphider
nt seit	entdeckt am 17. Juni 2010
nft	USA, Israel (unbestätigt)
	Netzwerkwurm

Stuxnet-Trojaner

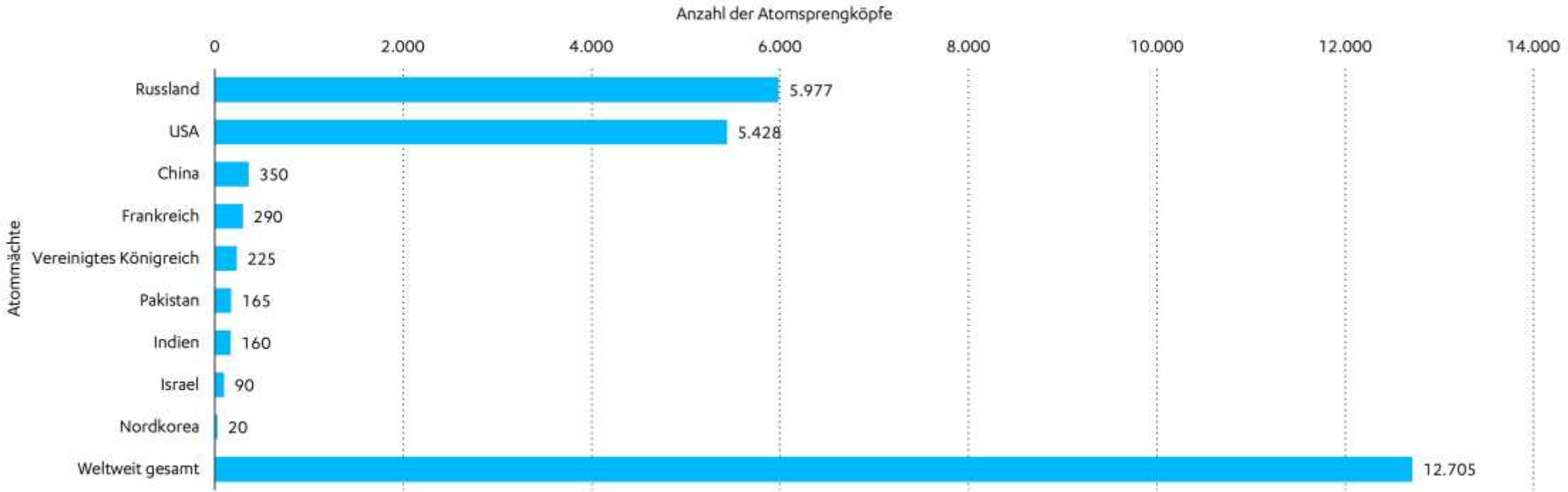
tdeckt am 17. Juni 2010

SA, Israel (unbestätigt)

tzwerkwurm

ANZAHL DER ATOMSPRENGKÖPFE WELTWEIT 2022

Anzahl der nuklearen Sprengköpfe weltweit 2022 (Stand: Januar 2022)



Hinweis: Weltweit

Weitere Angaben zu dieser Statistik, sowie Erläuterungen zu Fußnoten, sind auf Seite 8 zu finden.

Quelle: SIPRI ID 36401

BASIS: Schwachstellen

WITH secure

svbl 💙💛
@svblxyz

Russian military leadership. I might use these photos in my next Cyber Security presentation. 😬

Tweet übersetzen

10:48 vorm. · 3. Mai 2022 · Twitter Web App

1.283 Retweets **366** Zitierte Tweets

HACKBACK

WITH secure

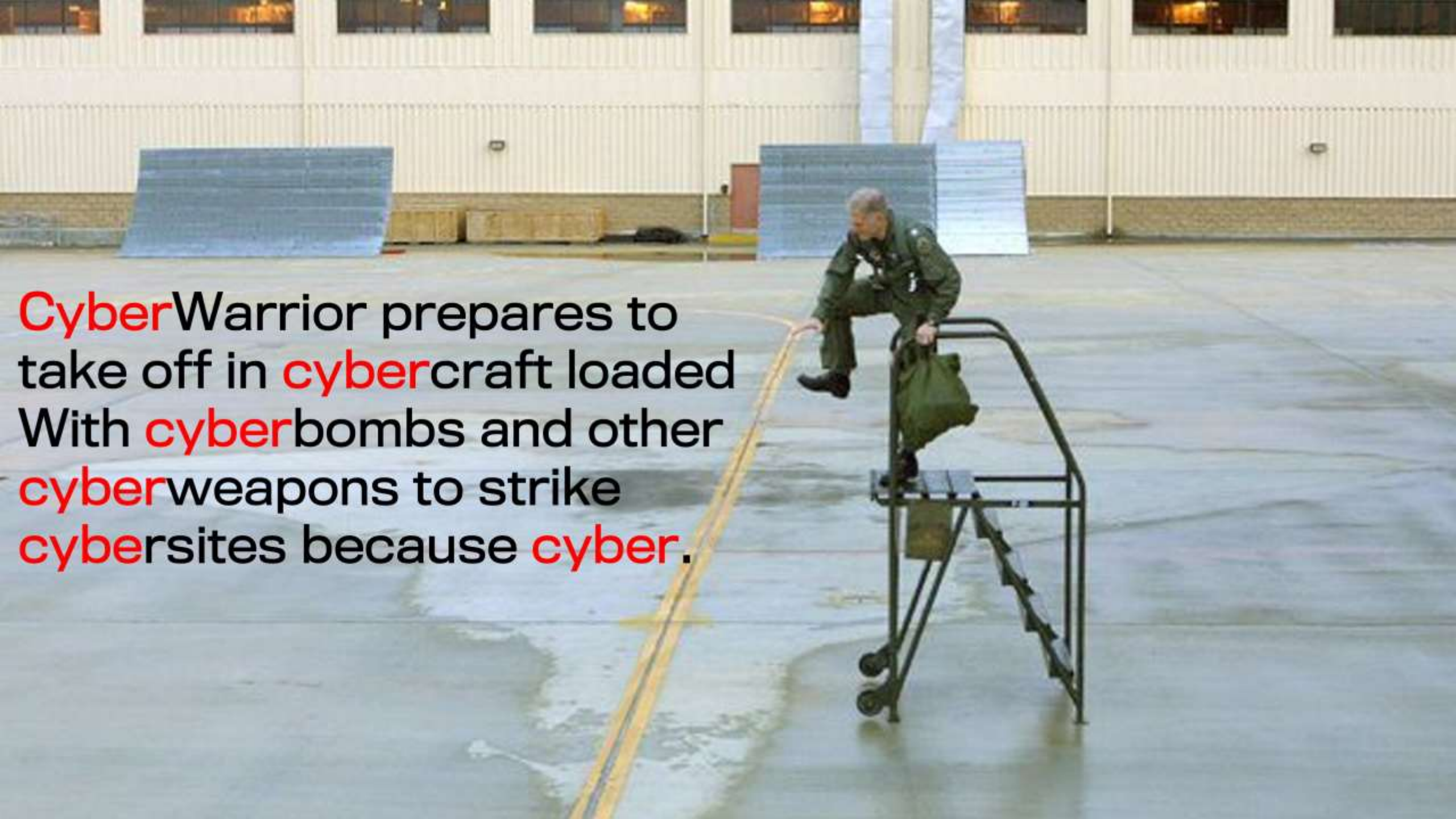
isteinhackbackeineguteidee.de

W/TH secure

NEIN

NEIN

NEIN


CyberWarrior prepares to
take off in cybercraft loaded
With cyberbombs and other
cyberweapons to strike
cybersites because cyber.

WINDOWS 7

CONTI

CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

Search

Web mirror

Tor mirror

"GERSHMAN MORTGAGE"

http://www.gershman.com

Headquarters:
6 Tesson Ferry Rd, St. Louis,
ouri, 63128, United States
ne

ne:

"EXAIR"

http://www.exair.com

11510 Goldcoast Dr, Cincinnati, Ohio, 45249, United States

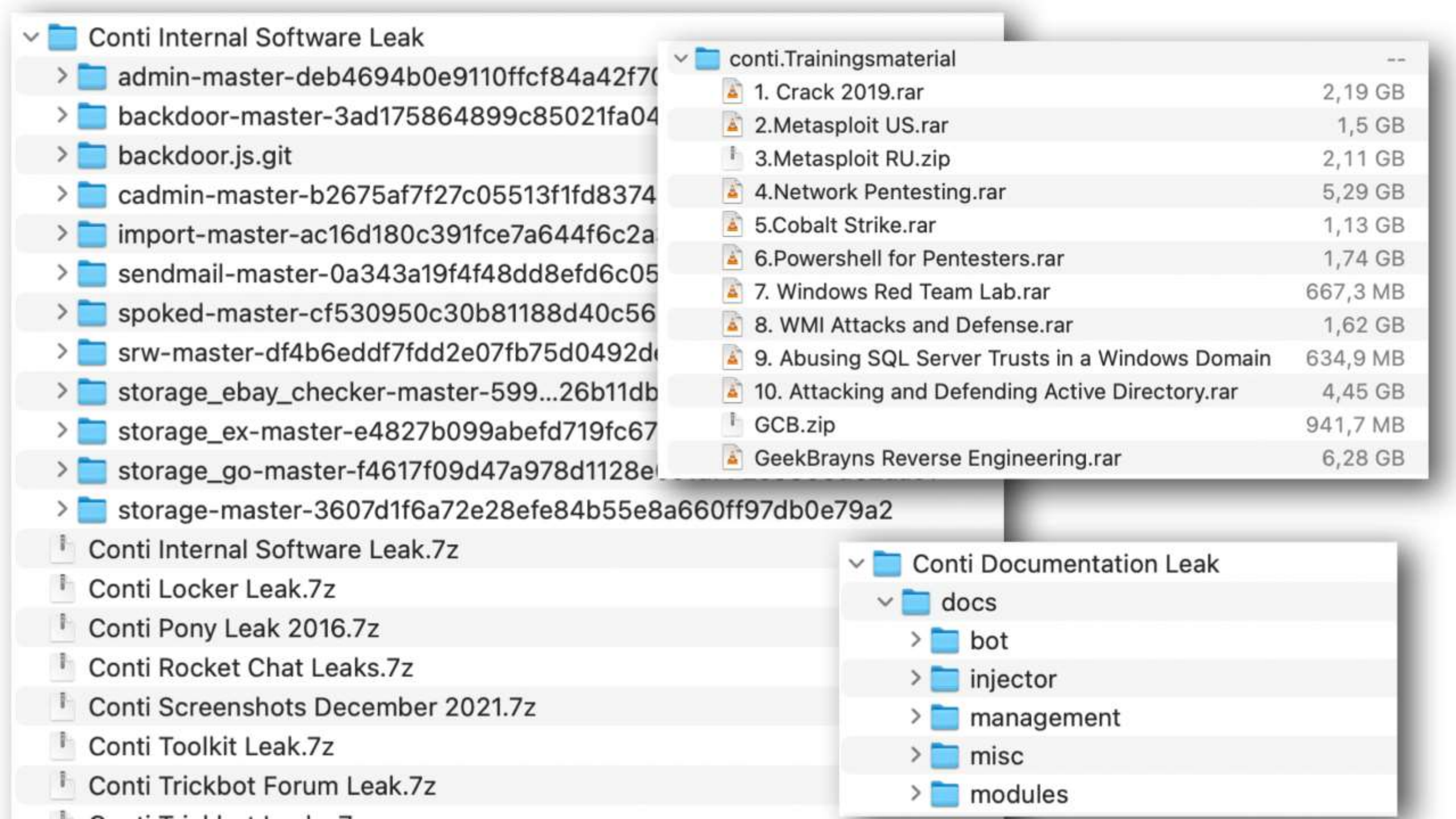
EXAIR Corporation was incorporated in 1983 as a manufacturer of compressed air-operated products to solve problems in industrial plants. Our product line includes

"JASEC"

https://jasec.go.cr

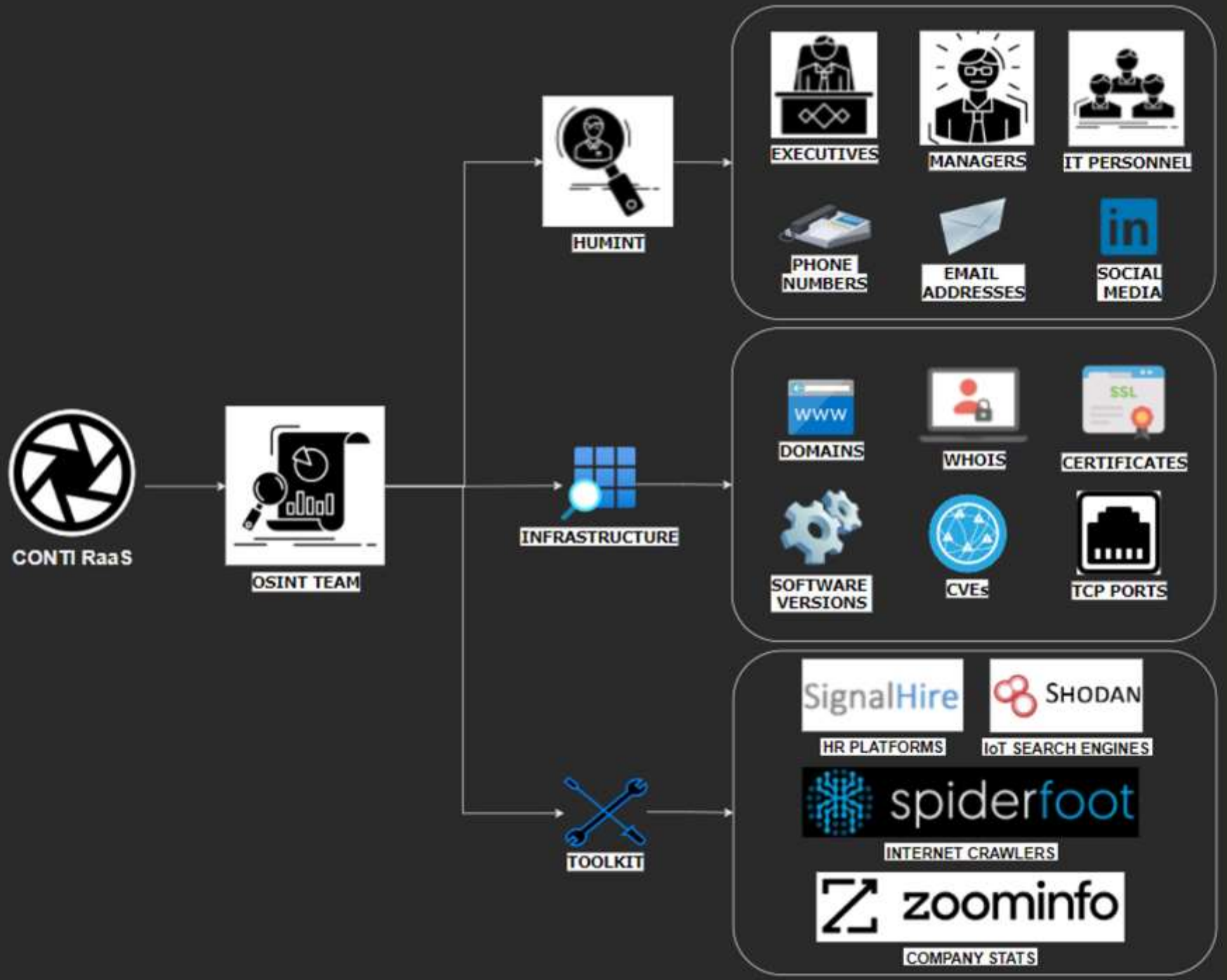
Avenida 2, Cartago, Cartago, Costa Rica

Una empresa corporativa de servicios de interés público, líder, visionaria, con calidad internacional, que supera las expectativas de los clientes


Conti Internal Software Leak
admin-master-deb4694b0e9110ffcf84a42f7
backdoor-master-3ad175864899c85021fa04
backdoor.js.git
cadmin-master-b2675af7f27c05513f1fd8374
import-master-ac16d180c391fce7a644f6c2a
sendmail-master-0a343a19f4f48dd8efd6c05
spoked-master-cf530950c30b81188d40c56
srw-master-df4b6eddf7fdd2e07fb75d0492d
storage_ebay_checker-master-599...26b11db
storage_ex-master-e4827b099abefd719fc67
storage_go-master-f4617f09d47a978d1128e
storage-master-3607d1f6a72e28efe84b55e8a660ff97db0e79a2
Conti Internal Software Leak.7z
Conti Locker Leak.7z
Conti Pony Leak 2016.7z
Conti Rocket Chat Leaks.7z
Conti Screenshots December 2021.7z
Conti Toolkit Leak.7z
Conti Trickbot Forum Leak.7z
conti.Trainingsmaterial --
1. Crack 2019.rar 2,19 GB
2.Metasploit US.rar 1,5 GB
3.Metasploit RU.zip 2,11 GB
4.Network Pentesting.rar 5,29 GB
5.Cobalt Strike.rar 1,13 GB
6.Powershell for Pentesters.rar 1,74 GB
7. Windows Red Team Lab.rar 667,3 MB
8. WMI Attacks and Defense.rar 1,62 GB
9. Abusing SQL Server Trusts in a Windows Domain 634,9 MB
10. Attacking and Defending Active Directory.rar 4,45 GB
GCB.zip 941,7 MB
GeekBrayns Reverse Engineering.rar 6,28 GB
Conti Documentation Leak
docs
bot
injector
management
misc
modules

```
{
  "ts": "2021-06-04T05:42:17.041982",
  "from": "derek@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "and today we will infect 4k computers with Twin with a trick, since State institutions do not pay, we will display the
information and instead of a locker we will upload it to all machines in the trickbot network so that staffers can make a profit"
}
{
  "ts": "2021-06-04T05:42:53.790702",
  "from": "derek@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "About xerox, Ali says it is difficult, but the prospects are good"
}
```

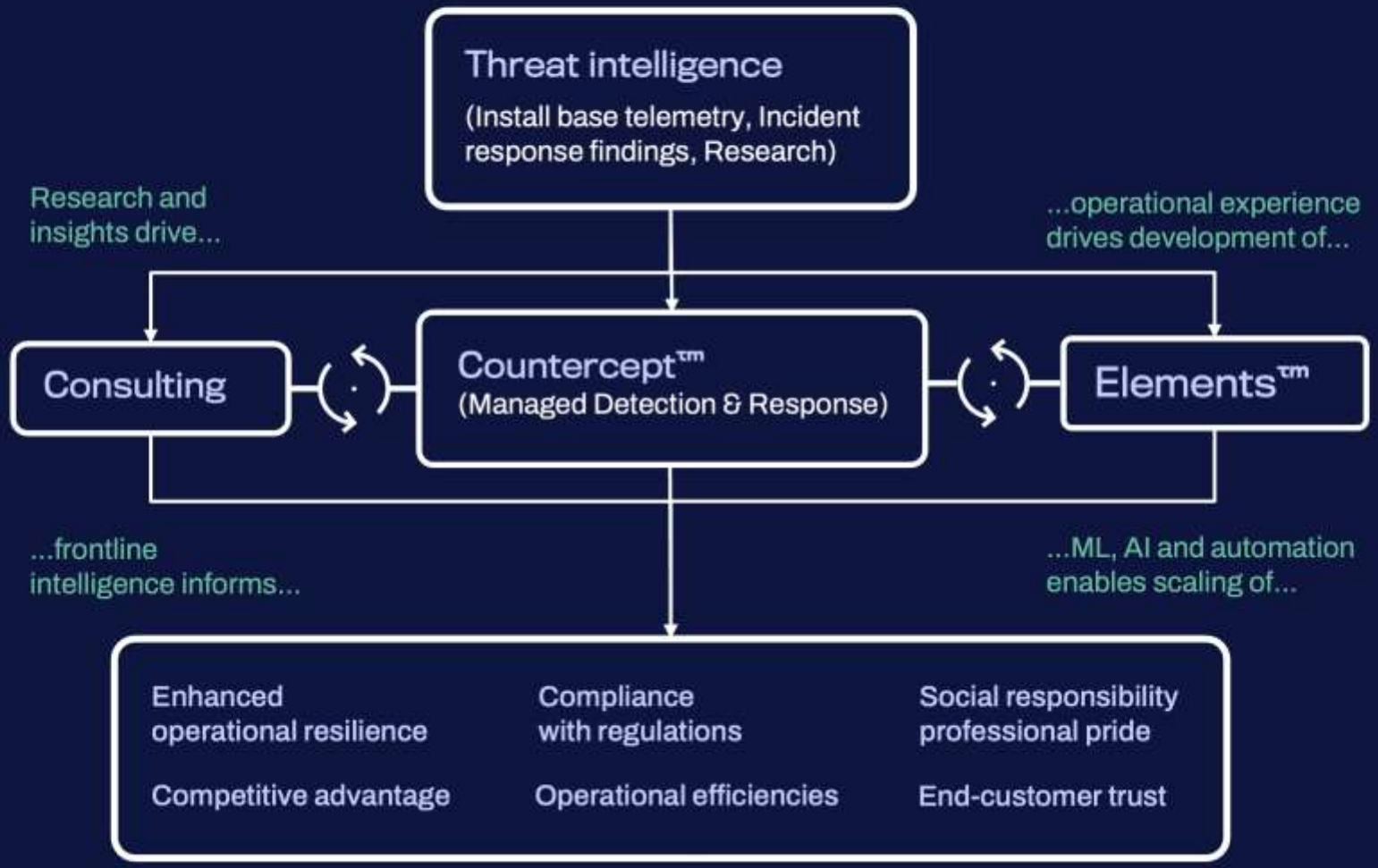
```
{
  "ts": "2021-01-29T14:19:43.943814",
  "from": "lemur@q3mcco35auwcstmt.onion",
  "to": "hash@q3mcco35auwcstmt.onion",
  "body": "and then the awl is generally empty"
}
{
  "ts": "2021-01-29T14:21:41.586680",
  "from": "carter@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "\n\nearlier it came out due to new orders, there were several for rocco and alexis, brooks ordered vpski more, vpn
alexis, I also wanted to know if it is possible to take a small vacation for 4 days at all, I need to decide with the documents at
home, but I will still come in daily"
}
{
  "ts": "2021-01-29T15:19:40.874614",
  "from": "defender@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "OK"
}
```


CONTI RaaS
OSINT TEAM
HUMINT
INFRASTRUCTURE
TOOLKIT
EXECUTIVES
MANAGERS
IT PERSONNEL
PHONE NUMBERS
EMAIL ADDRESSES
SOCIAL MEDIA
DOMAINS
WHOIS
CERTIFICATES
SOFTWARE VERSIONS
CVEs
TCP PORTS
SignalHire
HR PLATFORMS
SHODAN
IoT SEARCH ENGINES
spiderfoot
INTERNET CRAWLERS
zoominfo
COMPANY STATS

WITH secure

Was können wir tun?

Co-security within our business



WITH secure

Halle 6, Stand 6-220

WITH secure

Halle 6, Stand 6-220

WITH secure

Halle 6, Stand 6-220

WITH secure

Halle 6, Stand 6-220

WITH secure

Halle 6, Stand 6-220