



Protecting your Cyber Blind Side through Proactive Supply Chain Security

Mark Jaster
Founder & CEO
418 Intelligence Corp.

mark@418intelligence.com

Mark Jaster - Biography



- **Founder and CEO, 418 Intelligence Corp.**
- Reston Virginia based innovator in proactive cyber defense and workforce development.
- Over 30 yrs of experience in technology in cybersecurity, national security, space and private industry.
- Former USAF Officer, NASA manned space mission manager, and expert in medical devices, banking systems and intelligence systems.
- Founded 418 Intelligence to commercialize technology developed for the US Intelligence Community to create collective and proactive cybersecurity for underserved entities in critical sectors without requiring network or desktop technologies.

Context: Attackers don't have to hack into systems today, when they can just buy your LOGINs for \$10.00 on the Dark Web!

INFOSTEALERS ARE SURGING!



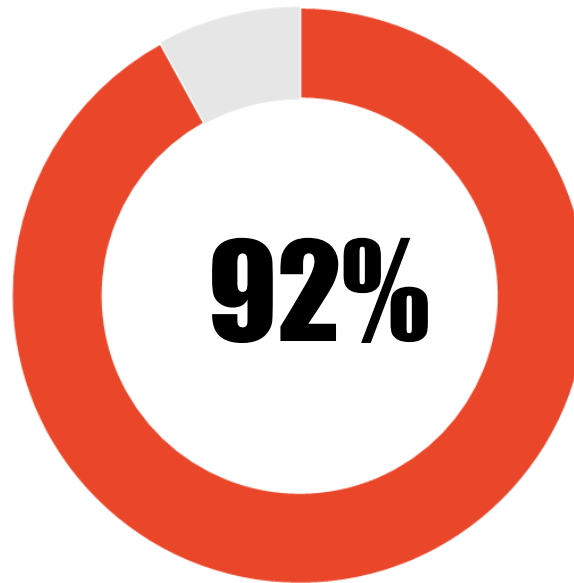
**Up 180%
since 2023**



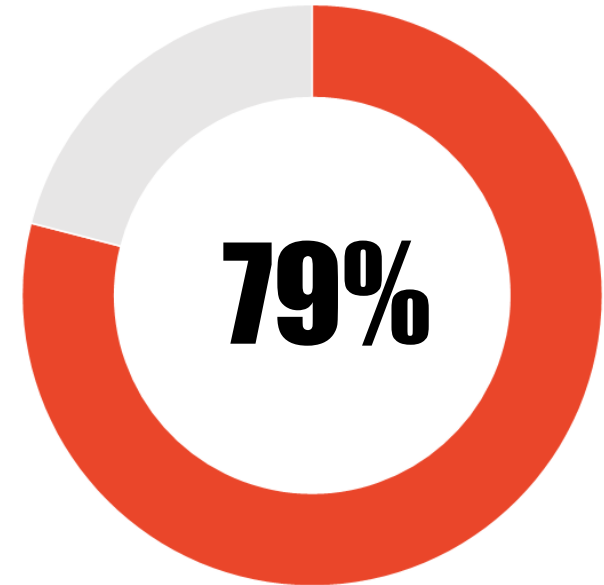
**#1 threat (30%
Overall)**



**32M hacked
machines**



INFOSTEALERS Dominated the Top 25 Breaches of the Past Year



The same was true for Web Breaches Overall

How Infostealers work



Municipalities and trusted vendors are top targets because you are easy marks for high-dollar invoice fraud and ransomware.

City of Fort Lauderdale loses \$1.2 million in phishing scam, police in Florida say

By Jamiel Lynch, CNN
2 minute read · Published 1:56 AM EDT, Sun September 24, 2023



\$1,200,000

Fort Lauderdale City Hall. John McCall/South Florida Sun Sentinel/Tribune News Ser

Massachusetts Town Loses \$446,000 in Cyber Attack

By Andrew G. Simpson | June 12, 2024

Subscribe to Newsletter

\$446,000

of Arlington reports it has lost \$445,945 in funds intended for a high school building project that were instead diverted to wire fraud scam.

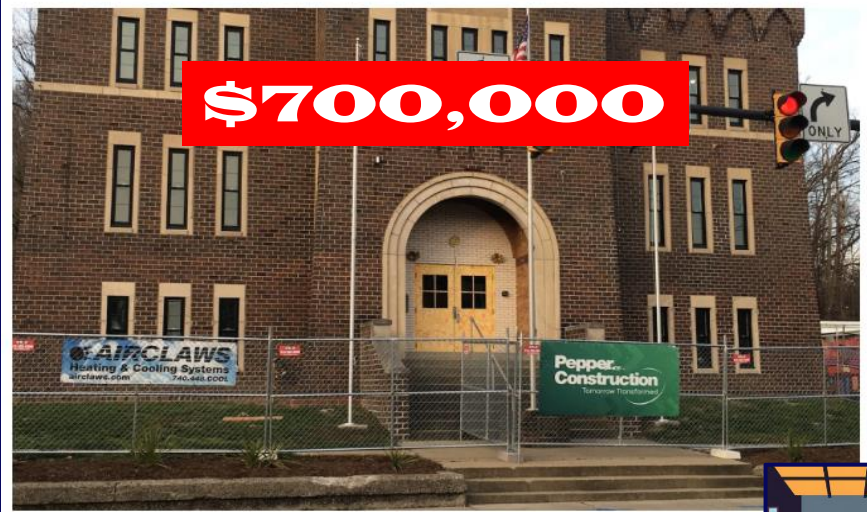
They alerted the public that the cyber criminals obtained the town as a business email compromise (BEC) using phishing, and compromised email accounts to commit the w



Cyber scams are taking a toll on small town Ohio

The Ohio Newsroom | By Erin Gottsacker
Published April 3, 2025 at 4:47 AM EDT

▶ LISTEN · 4:30



\$700,000

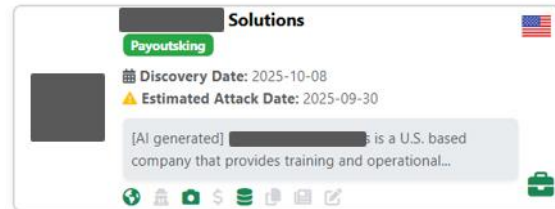
Pepper Construction is the contractor for the remodeling of the Army in Athens. The city was recently the victim of a cyber crime by s pretending to be a representative of the contractor.



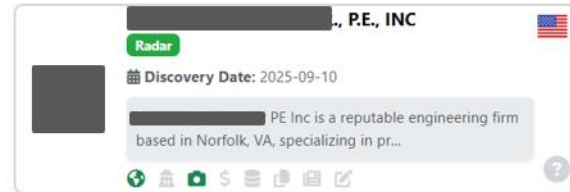
Recent Relevant Virginia Ransomware Victims (Redacted)

Virginia Municipal Supply Chain Ransomware Victims

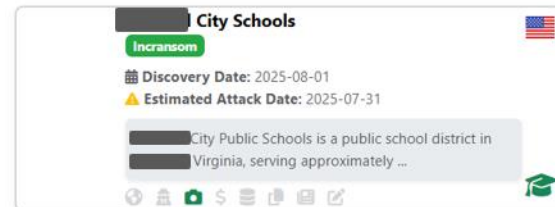
VA Beach IT Vendor
10/8/2025



Norfolk Engineering Svcs
9/10/2025



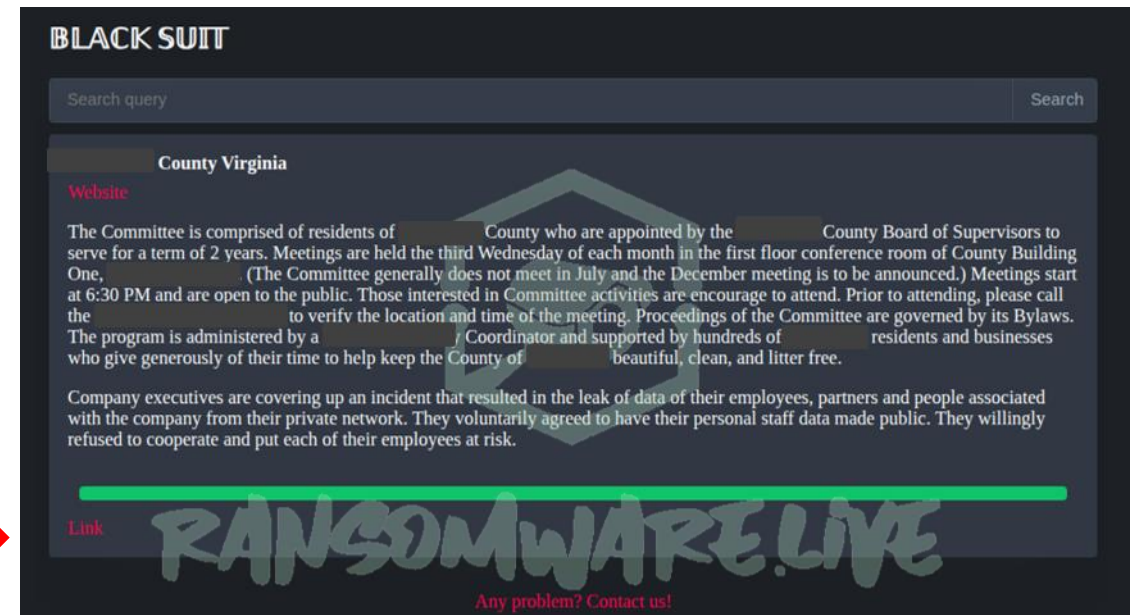
Blue Ridge Region K12
8/1/2025



Chesapeake Bay Area Govt
5/15/2025



Attacker's Ransomware Listing



Turning the tables.

A City in Virginia compromised on 10/1/2025

The dashboard provides a comprehensive overview of system security. At the top, a summary bar displays key metrics: 61 Total Stealers, 10 Compromised Employees, 5 Third Party Credentials, 51 Compromised Users, 0 Compromised App Users, 4+ External Domains, and 41 External Attack Surface. Below this, a navigation bar includes a refresh icon, a time filter set to 'All Time', a 'Date Compromised' dropdown, a 'Filter by Keyword' input, and a 'FILTER' button.

The main content area is divided into two primary sections. On the left, a list of machines is shown, with the first entry highlighted. This entry details a machine with ID [redacted], identified as a 'Generic Stealer'. It lists the IP address [redacted], malware path as 'Not Found', and provides timestamps for the date compromised (2025-09-22 21:21:00) and the latest detection (2025-10-01 00:01:44). A yellow 'Unlock' button is present next to the machine ID.

The right section, titled 'Profile', provides a detailed view of the selected machine. It includes fields for Computer Name, Operating System (Windows 10 22H2 build 19045 (64 Bit)), Anti Virus (Not Found), Facebook (Not Found), and Virtualization (Directory). A red circle highlights the 'Initial Detection' timestamp of 2025-10-01 00:01:44. Below this, the 'Applications' section shows 'adfs' as the primary application, with a link to 'AI Attack Scenarios'. The 'Installed software' section displays icons for various applications, including Windows Store, Edge, and others, with a 'View' button.

The bottom section, 'Corporate Credentials Found: 1', displays a table of credentials. The first entry shows a URL 'https://fs.[redacted].gov/adfs/ls', a login field, a password field, and a password strength indicator labeled 'Weak'.

Is this really risky? ... **Very!**

AI Attack Scenarios

ADFS

A hacker gains unauthorized access to the ADFS server, allowing them to manipulate authentication processes. By doing so, they can perform man-in-the-middle attacks to intercept user credentials and gain unauthorized access to various systems and resources within the company.

Machine ID: [redacted]
Stealer Family: G...
IP Address: [redacted]
Malware Path: No...
Date Compromised: [redacted]
Latest Detection: [redacted]

Machine ID: [redacted]
Stealer Family: L...
IP Address: [redacted]
Malware Path: No...
Date Compromised: [redacted]
Latest Detection: [redacted]

Machine ID: [redacted]
Stealer Family: L...

https://fs.[redacted].gov/adfs/ls

Weak

How did it happen? ... The Blind Side smoking gun.

The screenshot displays a security dashboard with a top navigation bar containing several metrics:

- Total Stealers: 61
- Compromised Employees: 10
- Third Party Credentials: 5
- Compromised Users: 51
- Compromised App Users: 0
- External Domains: 4+
- External Attack Surface: 41

Below the navigation bar, there is a list of compromised systems. The first system is highlighted with a yellow background and contains the following details:

- Machine ID: [redacted]
- Stealer Family: Generic Stealer
- IP Address: [redacted]
- Malware Path: Not Found
- Date Compromised: 2025-09-22 2
- Latest Detection: 2025-10-01 00:3

Below this, there is a list of installed applications. The applications are listed in a table with columns for the application name and its version/manufacturer. The applications are:

- Denuvo Anti-Cheat (6.7.0.8498) - Denuvo Gm
- Epic Games Launcher (1.0.0.0) - Epic Games, Inc. - C:\Downloads\ - 202509
- Microsoft OneDrive (25.170.0901.0002) - Microsoft Corporati
- Launcher Prerequisites (x64) (1.0.0.0) - Epic Games, In
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.44.35211.0] - Microsoft Corporati
- Microsoft Edge WebView2 Runtime (140.0.3485.81) - Microsoft Corporation - 202509
- Steam (2.10.91.91) - Valve Corporati

Red circles highlight the following applications: Denuvo Anti-Cheat, Epic Games Launcher, and Steam. A red arrow points from the Epic Games Launcher entry to the Downloads folder path in the file system view on the right.

At the bottom of the dashboard, there is a section for URL, Login, Password, and Password Strength. The URL field contains the text: https://fs.[redacted].gov/adfs/ls. The Password Strength indicator shows a red bar and the word "Weak".

418 DEF3NSE™ de-risks cities and supply chains collectively to stop new threats through monitoring & AI.

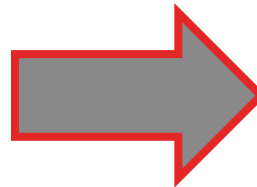
1: Identify Unknown & Unseen Risks

INITIAL SUPPLY CHAIN RISK ASSESSMENT *

ASSESS & MITIGATE CURRENT STATE RISK

1. Analyze unseen risks to business from blind-spots (BYOD, Vendors, Third-parties).
2. Reveal insights from AI Risk Assessments.
3. Mitigate & advise on identity monitoring options.

** Initial quick look is free.*



2: Continuously Pre-empt High Risks

BASIC SMALL CITY PLAN MEDIUM CITY & COUNTY PLAN

REMEDiate & UPSKILL

Resolve compromised credentials.
Train & equip staff with AI for self-service.

MONITOR & MITIGATE

Monitor, preempt and mitigate new incidents across all
Key Identities. Provide **corrective** training.

REPORT MONTHLY

418 DEF3NSE™ Protects your Cyber Blind Side Proactively

MONTHLY REPORTING

- Employees
- Vendors / Customers
- Service Network

AI UPSKILLING & HARDENING

- AI self-service agent subscriptions
- MSSP Services (Partners)

HUMAN VULNERABILITIES

- Corrective trainings
- Real-time VIP Monitoring



TRIAGE RISK ASSESSMENTS

- Vendor/Supply Chain Integrated
- 90% AI Native
- "Instant" turnaround

REAL-TIME MONITORING

- Annual Subscription
- Same/Next-day Detection

INVESTIGATIONS

- Intelligence driven
- AI Self-Service

Limited Free Student Externship Trial Opportunity

MONTHLY REPORTING

- Employees
- Vendors / Customers
- Service Network

AI UPSKILLING & HARDENING

- AI self-service agent subscriptions
- MSSP Services (Partners)

HUMAN VULNERABILITIES

- Infostealer Awareness Videos



TRIAL RISK ASSESSMENTS

- IT or HR Vendor
- 3rd-Party Platform (e-Permitting)
- Key individuals

REAL-TIME MONITORING

- Annual Subscription
- Same/Next-day Detection

INVESTIGATION DEMO

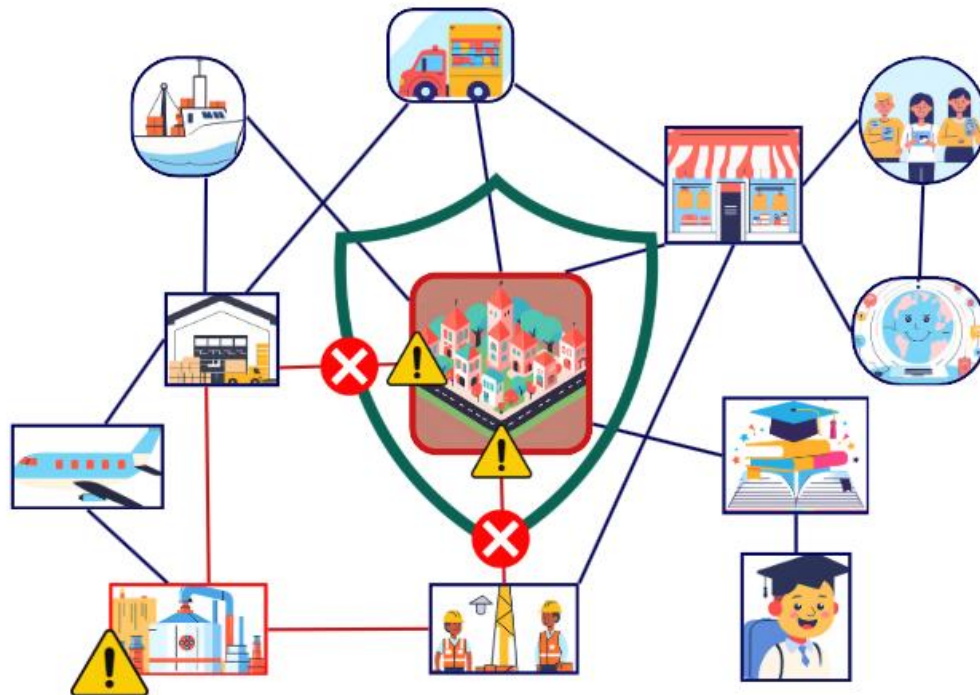
- Intelligence driven
- AI Self-Service

Program to Phase-in Municipal **Collective** Defense

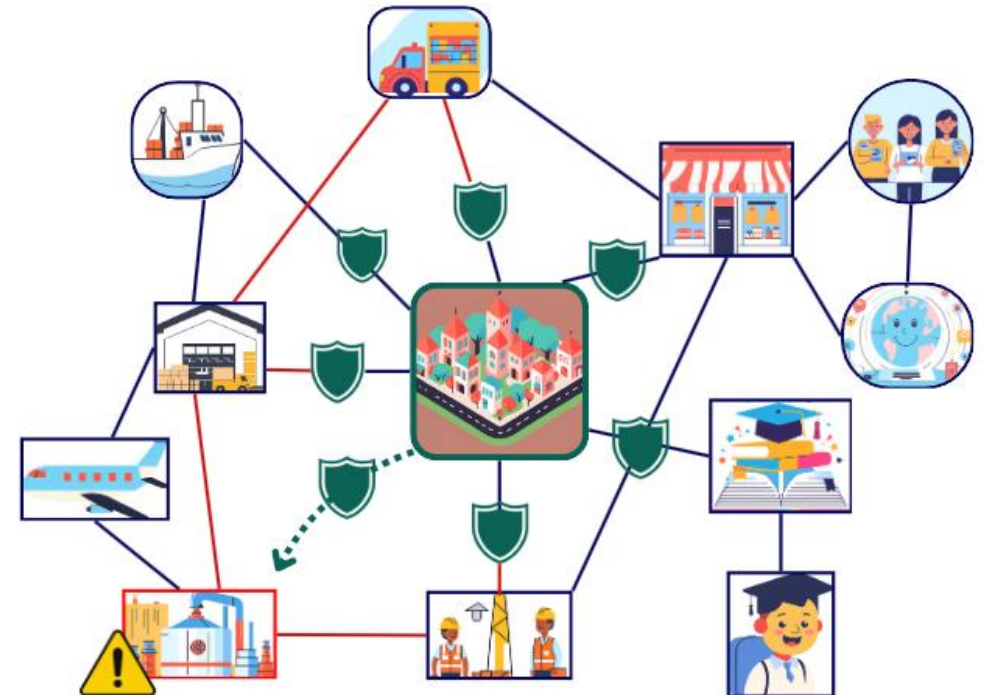
- 6-month Virginia Veteran SkillBridge Internships in 6-city clusters
- Security risk management assessments
- Supply chain focus on capital improvement projects and critical infrastructure
- Strategic vendor monitoring for collective benefit
- \$2,000 per month per city + annual \$7,500 for IT dept. AI training & use
- Launch target of 18 cities (3 interns / clusters)

Supply chain weak links can be stopped from putting your community's data, people and payments at risk.

Bypassed Defenses Puts **All Budgets at Risk**



Solution: AI Proactive Defense of City Supply Chains



If nothing else... At least learn about October's latest Supply Chain attacks

- **"Payroll Pirates" Stealing Employee Salaries from HR SaaS Platforms**
<https://thehackernews.com/2025/10/microsoft-warns-of-payroll-pirates.html>
- **Oracle Software Bug Used in Major Multi-Vendor File Transfer Campaign**
<https://thehackernews.com/2025/10/cl0p-linked-hackers-breach-dozens-of.html>
- **RedHat Supply Chain Data Breach Affects 800 Critical Enterprises**
<https://www.thecipherbrief.com/red-hat-breach>



Let's stop cyber crime together.

Mark Jaster, Founder & CEO

mark@418intelligence.com