AGC
THE CONSTRUCTION
ASSOCIATION

# 7 Things That Construction Companies Were Doing Wrong That Got Them Hacked

Terry Bradley

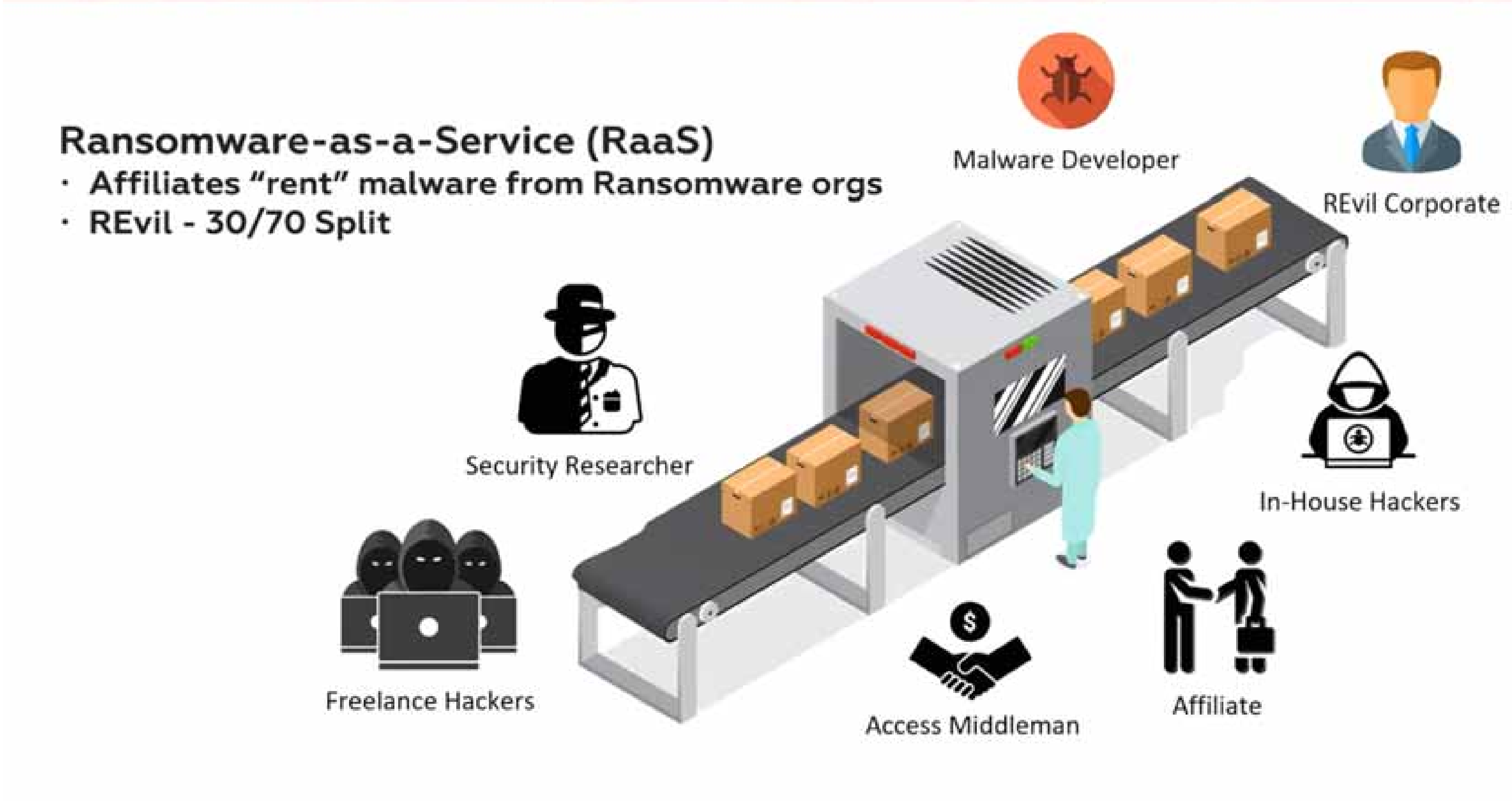
Mile High Cyber

2025 AGC Technology Conference

- 30+ years working in “cyber:”
  - Air Force / NSA
    Early days of “cyber”
  - U.S. Cyber Command
    Network Attack Planner
  - Booz Allen Hamilton
    Red Team Manager
- Working to help SMBs with cybersecurity since 2015

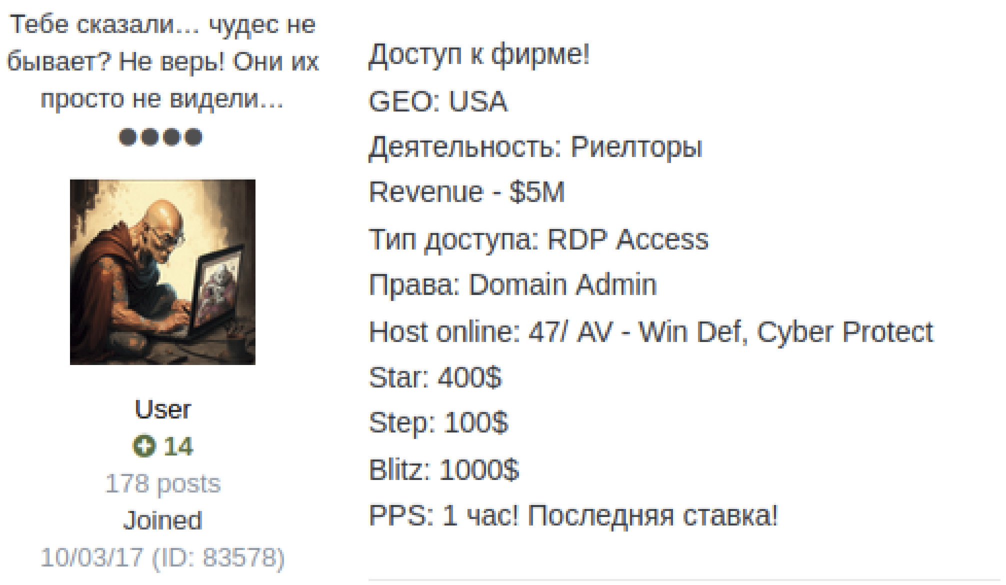
# Misconception

# Teams of Hackers



## Ransomware-as-a-Service (RaaS)

- Affiliates "rent" malware from Ransomware orgs
- REvil - 30/70 Split



Тебе сказали… чудес не бывает? Не верь! Они их просто не видели…

●●●●

User

⊕ 14

178 posts

Joined

10/03/17 (ID: 83578)

Доступ к фирме!

GEO: USA

Деятельность: Риелторы

Revenue - $5M

Тип доступа: RDP Access

Права: Domain Admin

Host online: 47/ AV - Win Def, Cyber Protect

Star: 400$

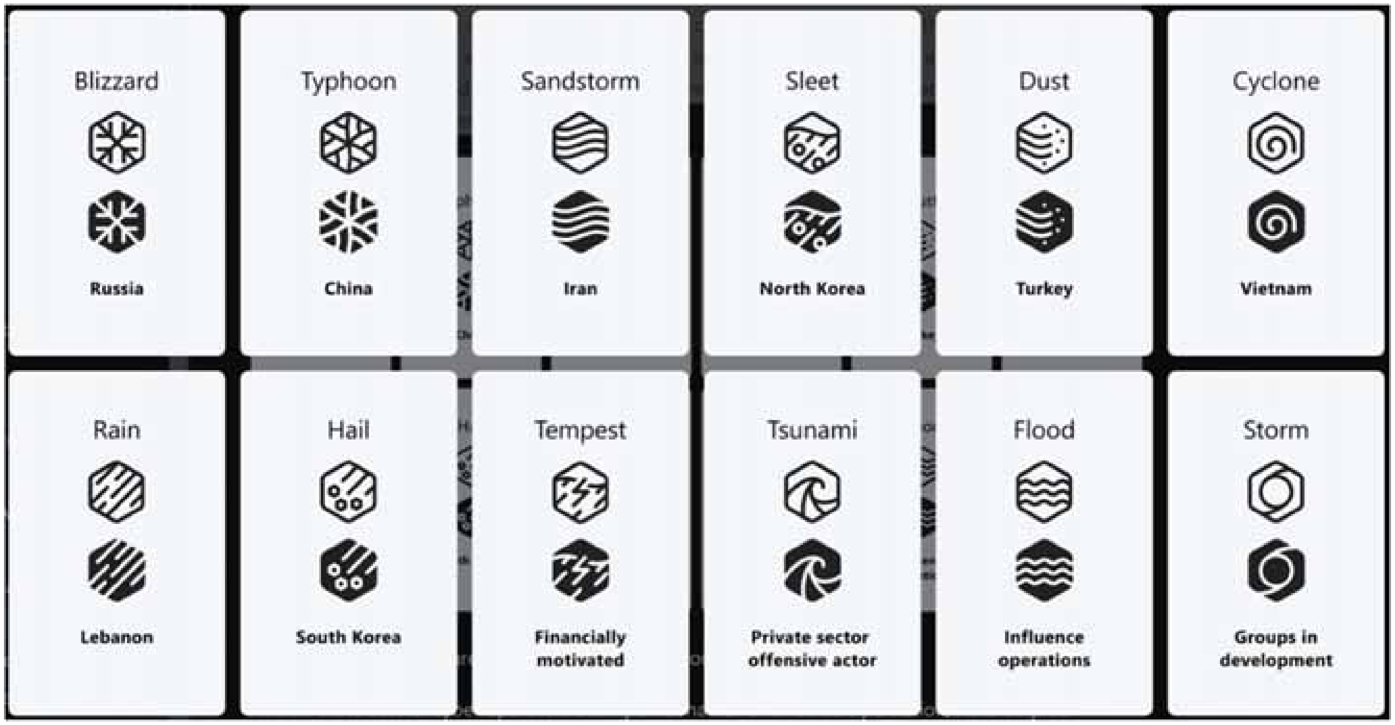
Step: 100$

Blitz: 1000$

PPS: 1 час! Последняя ставка!

## Initial Access Broker

- Geographic Location (USA)
- Victim revenue ($5M)
- Access method (Remote Desktop Protocol)
- Privilege level (Domain Admin)
- Price: $1000 to buy it now!



Blizzard
Russia

Typhoon
China

Sandstorm
Iran

Sleet
North Korea

Dust
Turkey

Cyclone
Vietnam

Rain
Lebanon

Hail
South Korea

Tempest
Financially motivated

Tsunami
Private sector offensive actor

Flood
Influence operations

Storm
Groups in development

Microsoft Threat Intelligence Taxonomy

# 7 Things That Got Construction Companies Hacked

## Remote Access with no Multi-factor Authentication (MFA)

- Remote Desktop Protocol (RDP)
- GoToMyPC
- PCAnywhere
- TeamViewer
- Etc.

## Failed to apply security updates

- Log4j remote code execution (Log4Shell)
- Palo Alto RCE (Midnight Eclipse)
- MOVEit SQLi RCE
- Apache Tomcat RCE (CVE-2025-24813)
- Citrix NetScaler RCE (CitrixBleed 2)

## Did not change default passwords

- Admin / admin
- Admin / 12345
- Admin / 123456
- Admin / Password
- Search set-up guide for “password”

- **HOT ATTACK: Printer configuration pages**

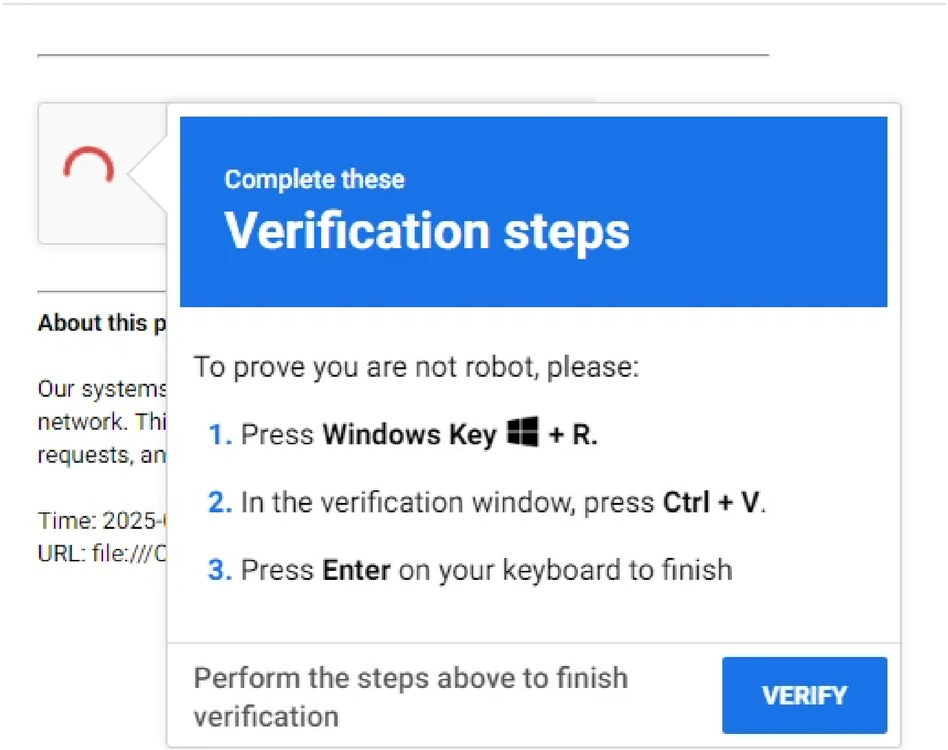
## Phishing / Infostealers

- Fake login pages connected to reverse proxy servers to steal passwords and MFA tokens
- Infostealers like malicious browser plug-ins or other drive-by downloads can also bypass MFA

- **HOT ATTACK: ClickFix & FileFix**

# ClickFix Attack

- Tricks user into running PowerShell script to download and run infostealers like LummaC2, RedLine, etc.
- What happens if your users run a PowerShell script?



About this p

Our systems
network. Thi
requests, an

Time: 2025-
URL: file:///C

Complete these
## Verification steps

To prove you are not robot, please:

1. Press **Windows Key** ⊞ **+ R.**
2. In the verification window, press **Ctrl + V**.
3. Press **Enter** on your keyboard to finish

Perform the steps above to finish verification

## Misconfigured cloud or office computers

- SMB Signing Not Required
- LDAP Channel Binding Not Enforce
- Machine account quota (MAQ) = 10
- Scanner account with no MFA
- M365 Direct Send enabled

AGC
THE CONSTRUCTION ASSOCIATION

## Third-party / Supply-chain compromise

- Target 2013
- SolarWinds 2021
- Change Healthcare 2024
- Snowflake 2024
- CDK 2024
- United National Foods Inc. 2025

## Lack of Employee Security Training

- Social engineering
- Accidental data leaks
- Creating and safeguarding strong passwords
- What hackers want
- What to do / who to call

1. Remote access VPNs without multi-factor authentication (MFA)
2. Failed to apply security updates (or legacy systems)
3. Did not change default passwords
4. Phishing / Infostealers
5. Misconfigured cloud or office computers
6. Third-party / Supply-chain compromise
7. Lack of Employee Security Training

# 3 Things You Can Do Now to Prevent Getting Hacked

## Enable and Enforce MFA Everywhere

- Strong passwords are not enough
- Multifactor Authentication needs to be enabled and enforced for all accounts
- New ways to bypass MFA are multiplying, but it is still a minimum security requirement

## Get EDR / MDR Monitored by Cyber Experts

- How do you know when you're being hacked?
- Endpoint Detection and Response software detects malicious activity on your computers and can block the bad activity
- MDR is Managed EDR software, monitored by a cybersecurity provider with a 24/7 security operations center
- Most cyber insurance companies require EDR/MDR and some even provide it as part of their coverage

## Test Your Security Protections

- Have an independent 3rd party test your network / applications
- Vulnerability Assessment
- Penetration Testing
- Red Teaming
- Purple Teaming
- Tabletop Exercises

- You won’t know until you’ve tested

1. Enable and Enforce MFA Everywhere
2. Get EDR / MDR Monitored by Cyber Experts
3. Test Your Security Protections

# Conclusion

- Most security incidents are preventable if you design a cybersecurity program around:
  - Prevention
  - Detection
  - Response
- Don’t wait to be a victim, stay ahead with available security protections and proactive testing

# Thank You!

Terry Bradley
719-310-5454
terry.bradley@milehighcyber.com

https://www.milehighcyber.com/contact-agc-2025