Coalition®

BROUGHT TO YOU IN PARTNERSHIP WITH BLACH CONSTRUCTION

Recovery Blueprint: An Interactive Ransomware Tabletop Exercise

Coalition Incident Response (CIR) and Blach

Table of Contents

Session Schedule: 8:30am-9:30am

YOUR TEAM

Chris Hendricks

Head of Coalition Incident Response (CIR)

Leeann Nicolo

Senior Incident Response Manager (CIR)

John Kern

Director of Information Technology (Blach)

Jon Saad

Senior Systems Engineer (Blach)

Scene Setting: Threat Landscape Trends

Motivation and context

Trends and Observations

Ransomware

USA is the top targeted country for Ransomware

accounting for 47% of victim organizations, followed by UK, Canada, Germany, & Italy

Industries with most incidents:

Manufacturing (21%), Professional Services (18%), Healthcare (6%), & Construction (5%).

Ransomware actors are becoming more vicious

They are also now going for “two bites at the apple” and DFIRs report seeing repeat attacks in short succession

Smaller organizations are not safe

Groups targeting orgs with revenue ~$50-60M. 31% of victims < $20M. High enough payouts, likely poorer security

Tabletop Exercise

Interactive and participatory

Today is the Day

Typical day

IT team among the first ones in the office, checking email and opening tickets submitted overnight

CTO arrives around 8AM

…bringing coffee and donuts for the staff since it's Friday

Employees arrive

…between 8:30AM and 9:30AM to begin their usual work day

Inject #1: Accounting Server Outage

What?

Employees begin calling in to the IT team that they are unable to access the Accounting server. The IT team attempts to access and confirms the outage.

When?

It's time for payroll: time is of the essence. The server has been offline for a few hours, the last connection to the monitoring service shows 4:07 AM local.

Why?

Unknown as to why the system is down at this time, the IT team works to restore the access for the most critical users.

Inject #1 Debrief

Questions for Consideration

- What groups within the organization would be involved in handling this event?
- What communications need to be sent around internally (externally?)
- How would these communications occur?
- What aspect of the response would be different if this was a different day or time (say over the weekend or a holiday)?

Inject #2: Ransomware Infection

What?

Upon further review, the IT team identifies files that can't be opened. They have file extension .23n9ushi and a README.txt in each directory with locked files.

When?

The first file with the updated file extension appears to have a timestamp of 8/6/24 at 11:30PM local.

Why?

It looks to be ransomware. In the ransom note, the threat actor states they are the "Akira" group. They demand $1.2M to unlock files and delete stolen data.

README.txt

Hi friends,

We have taken a great amount of your corporate data

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue.
1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralk3zq2dsrzsrvfh9r2xgbbu2wgsmx35jd4csgfameg52n7efvr2id.onion.
3. Use this code - 0714-LR-RMDF-DSJA - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

Inject #2 Debrief

Questions for Consideration

- What tools and resources would the team use in handling this incident?
- Could email be compromised? What other out of band communication channels can be set up to discuss how to deal with this?
- Do team members have the experience and/or support they need to remediate such an issue?

Inject #3: PR/Legal and TA Comms

T + 0m

What?

The threat actor starts calling employees. Threats are being made to SWAT the CEO, contact customers and DDoS the network so it's completely unusable.

When?

Nonstop! Can’t seem to get ahead of all the messages and calls from the threat actor.

Why?

Seems they are doing this to put pressure on us so that we pay them their ransom demand.

Inject #3 Debrief

Questions for Consideration

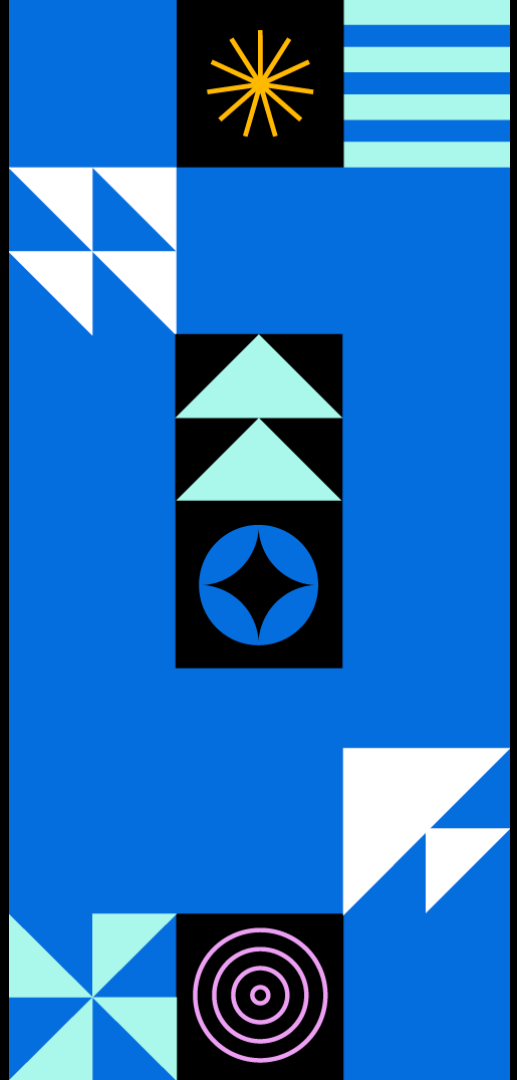
- Stolen data. What type of legal obligation do you have as a company to notify for such a breach?
- Do you have any public relations contacts to help communicate the event before it gets out there publicly by the threat actor directly?
- How does one even make a ransom payment?

Lessons Learned (Today)

Anything actionable?

Breached Organization Characteristics

Common threads and similarities across targets



Questions?

Thank You!

Advisory

You are advised to read this disclosure carefully before reading or making any other use of this presentation and related material. The content of this presentation is (i) not all-encompassing or comprehensive; (ii) solely for informational purposes; (iii) not be construed as advice of any kind or the rendering of consulting, financial, legal, or other professional services from Coalition; and (iv) not in any way intended to create or establish a contractual relationship. Any action you take upon the information contained herein is strictly at your own risk and Coalition will not be liable for any losses and damages in connection with your use or reliance upon the information. The content of this presentation may not apply directly to specific circumstances and professional advice should be sought before any action is taken in relation to the information disseminated herewith. Coalition makes no representation or warranties about the accuracy or suitability of information provided in the presentation or related materials. The presentation may include links to other resources or websites which are provided for your convenience only and do not signify that Coalition endorses, approves or makes any representation or claim regarding the accuracy of copyright compliance, legality, or any other aspects of the resources or websites cited.