
cisco Live!
ALL IN

The bridge to possible

The Past, Present and Future of Ransomware

Ankur Chadda,
Leader, Product Marketing - Cisco Secure
@ankur_chadda

Holger Unterbrink
Technical Leader, Engineering - Talos
@hunterbr72

PSOSEC-1020

Cisco Webex App

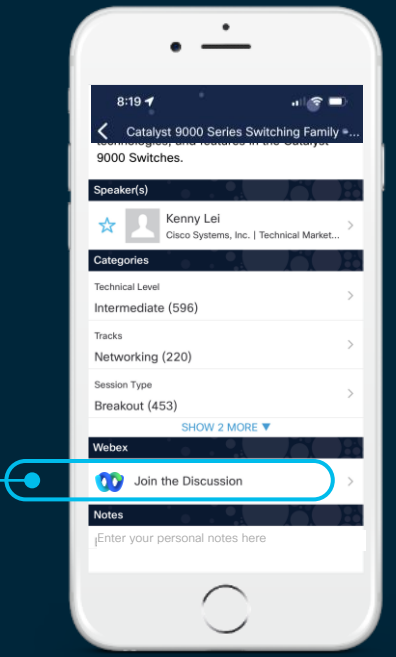
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.

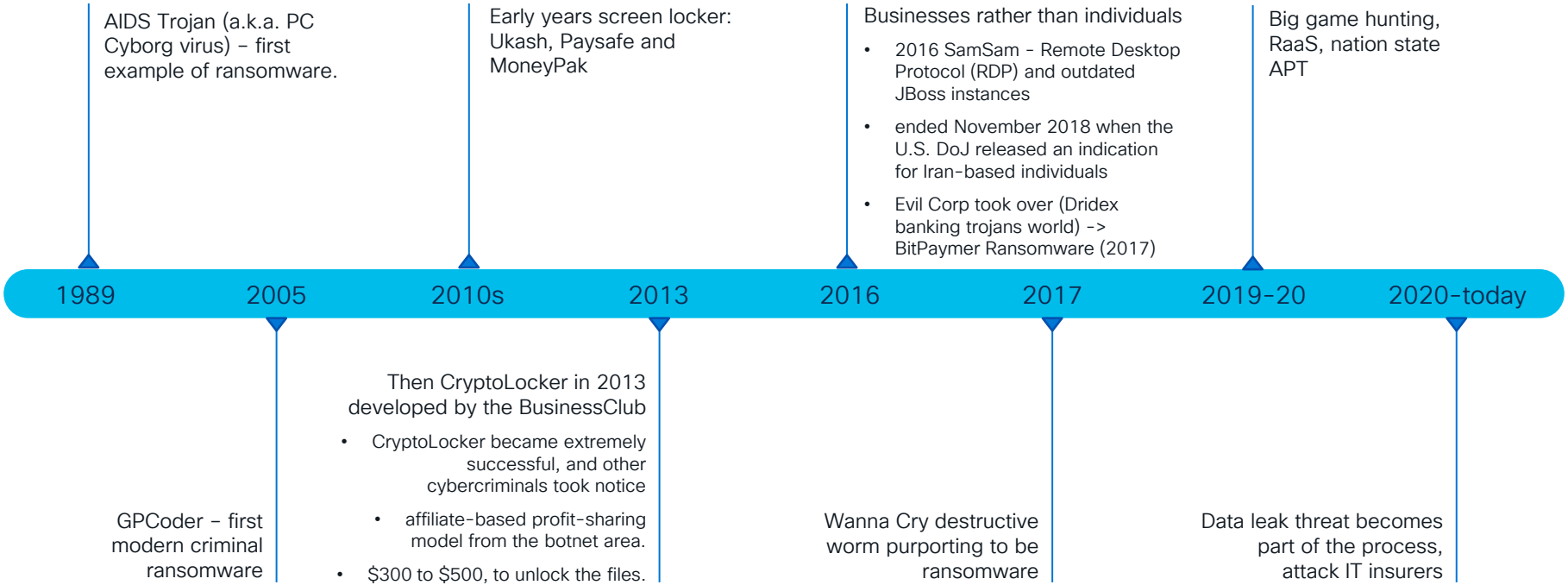


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXXX-xxxx

Agenda

- Ransomware past and evolution
- The ecosystem of ransomware
- Closer Look: How does REvil work?
- How do we protect ourselves?
- What should organizations do?
- Future outlook

Ransomware Evolution



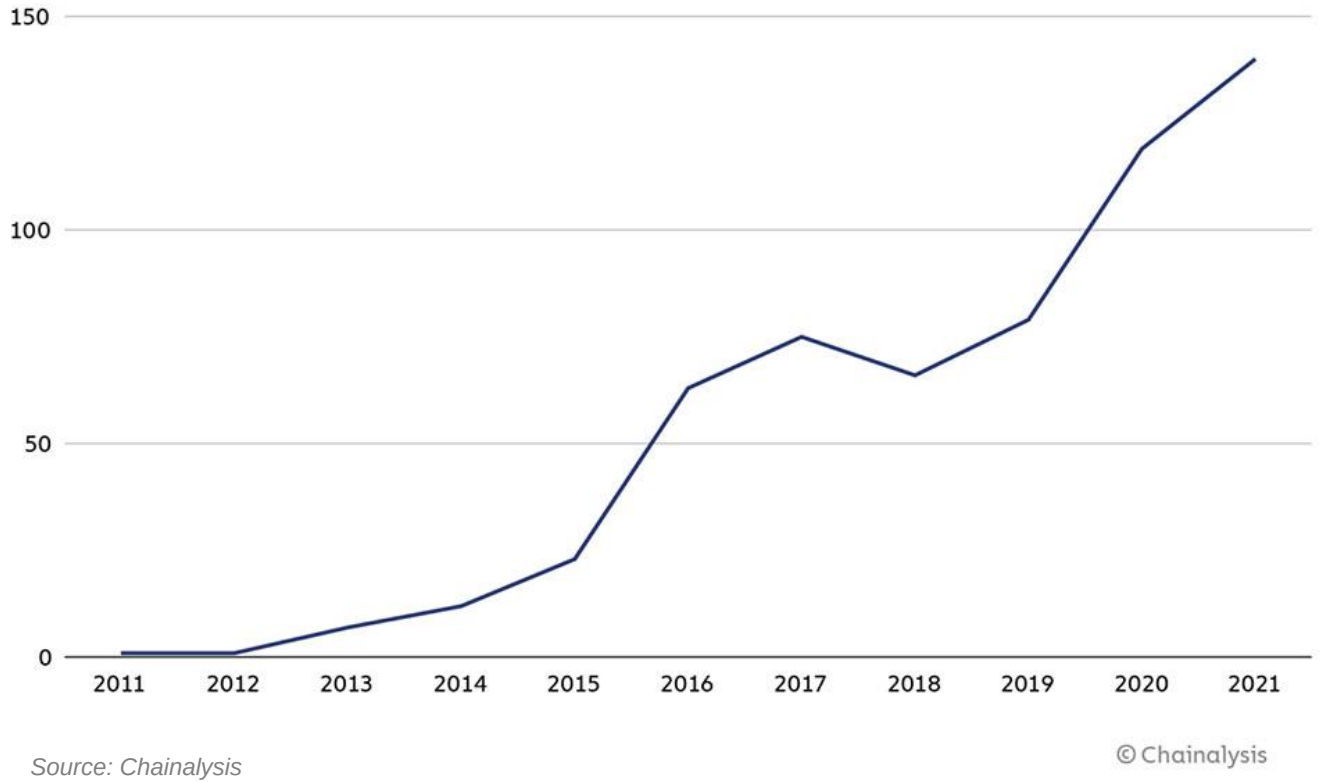
Ransomware evolution

- **1989 AIDS Trojan** (a.k.a. PC Cyborg virus) – first example of ransomware. Sending US$189 to a post office box in Panama
- **2005 GPCoder** – first modern criminal ransomware – eGold and Liberty Reserve digital currencies
- Early screenlockers: Ukash, Paysafe and MoneyPak
- Then, **CryptoLocker** in **2013** developed by the BusinessClub
  - CryptoLocker became extremely successful, and other cybercriminals took notice. The kickoff of today's ransomware business.
  - Affiliate-based profit-sharing model from the botnet
  - $300 to $500 to unlock the files - **$3 million revenue overall**

Ransomware evolution (cont.)

- **2016** Businesses rather than individuals
  - 2016: SamSam – Remote Desktop Protocol (RDP) and outdated JBoss instances
- **2017** Evil Corp took over (Dridex banking trojans world) -> BitPaymer Ransomware
- **2017** WannaCry destructive worm purporting to be ransomware
- **2018-20** RaaS, Big game hunting, nation state APT – GrandCrab/Revil, Lazarus group (VHD) - profit of $100 million each year
- **2020 – Present** Data leak threat becomes part of the process, attack IT insurers (CNA Financial (Phoenix CryptoLocker)

Active ransomware strains by year 2011 – 2021



Source: Chainalysis

The ecosystem of ransomware

Groups and affiliates (RaaS)

- **Botmasters** and **account resellers**: Initial access
- **Red team**: Lateral movement, gather information about the victim and steal internal documents
- **Analysts**: Who will try to figure out the actual financial health of the target, set the highest ransom price possible
- **Malware developers**: Sell ransomware software in the darknet
- **Negotiator/Money laundry**: As the name says

Example: How did REvil work?

- Init access: like RDP accesses, phishing, and software vulnerabilities
- Encrypt files
- Data leak extortion: Leak on the group's website (darknet leaks site)
- Voice calls to business partners and journalists
- CEOs are threatened with digital persecution
- Protection money

Do we know who the attackers are?

- Normal everyday people
  - IT admins, programmers, students
  - Talos Lockbit operator interview
- From petty criminals to organized crime syndicates
- Low-tech opportunistic criminals to elite hackers

How do we protect against ransomware?

- Should I pay or not?
  - Answer is not a straightforward yes or no.
  - “It depends” ☺
  - Local laws come into the picture
- Can I just let my insurance pay?
  - Maybe, but risky (Don't trust criminals)
  - AXA France for example excludes ransomware now!
  - Others will likely follow
- We need a technical solution

What should I be doing as an organization?

We need a multi-layered security architecture (defense-in-depth):

- User education
- Offline backups (not available for a single admin)
- 2FA/Biometric
- Patching: 1-days (rarely 0-day) are often used for first access (e.g., Microsoft Exchange vulnerabilities)
- Active scans to find existing bots and IOCs/Penetration tests
- Global incident response plans and tabletop exercises
- Attack simulations to test your processes

Future outlook

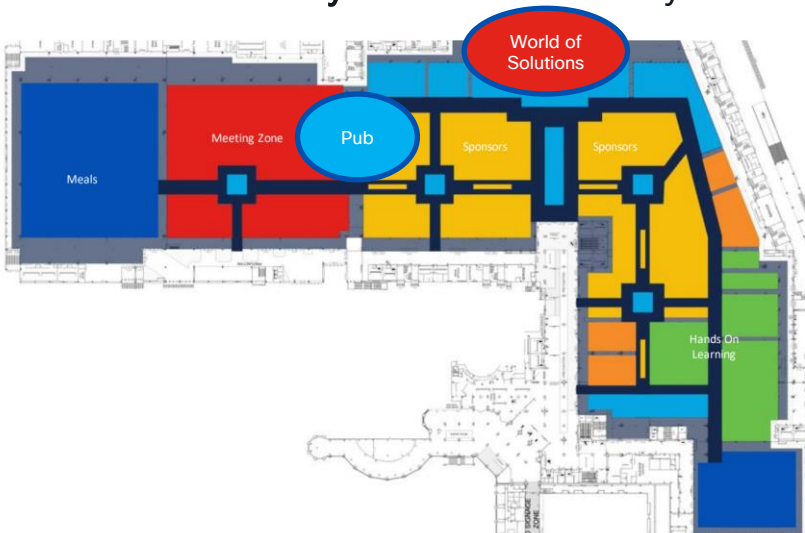
- Pandemic has certainly increased the bot count, actors might already have access to your network
- Attackers go against the low-hanging fruits. Most ransomware attacks are opportunistic.
- States are involved/perpetrators are protected
- Today's geopolitical situations can be a breeding ground
- Elite threat actors are starting to target firmware
  - Conti Leaks (LoJax, TrickBoot, MosaicRegressor,..)
  - UEFI/BIOS (SPI chip – firmware store), System Management Mode (SMM), Intel Management Engine (ME), AMT - CSME-Version-Detection-Tool

Customer Testimonials

- We would like to invite you to **share your thoughts, feedback, and experiences using our Cisco Secure products**. Your opinion is valued and could help others in their buying process.

- We will **have a team at the Cisco Secure Pub and World of Solutions – Security** area to assist you and you will have **full control and can edit or delete your review** at any time.

- We will be **wearing black t-shirts with "What's Your Story?"** printed on the front.



For more information, please reach out to

- **Cindy Valladares 503-784-8178**
- **Tazin Khan (she/her) (917) 602-6338**

cisco Live!

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

CISCO SECURE

Security Reference Architecture

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN