



ISOAG Meeting March 7, 2018

Welcome to CESC



Virginia Information Technologies Agency





Virginia Information Technologies Agency



Welcome and Opening Remarks

Michael Watson

March 7, 2018





ISOAG March 7, 2018

- | | |
|--|------------------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA. |
| II. Crypto Mining-What is it and How to protect against it? | Tom Arruda, Dominion Energy |
| III. Update on the progress of the COV and MITRE's launch of the VA Information Sharing Analysis Organization | Gabe Galvin, MITRE |
| IV. Google Messaging Transition Update | Jon Craft, VITA |
| V. Upcoming Events | Mike Watson, VITA |
| VI. Operations Update | NG |

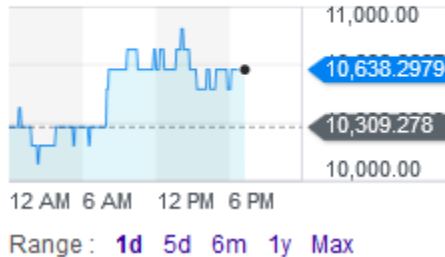
CryptoMining

What is it? How do I defend against it?

March 7, 2018

Cryptocurrency is all the rage

BTCUSD=X - BTC/USD CCY
News Charts Conversations



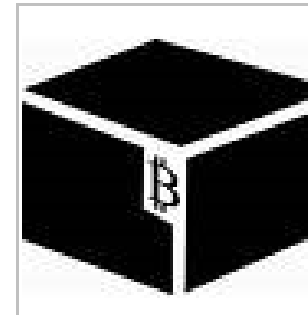
ethereum

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. **Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.** Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

Cryptominers are the new credit card companies



Cryptominers are the new credit card companies



Miners race to solve the block

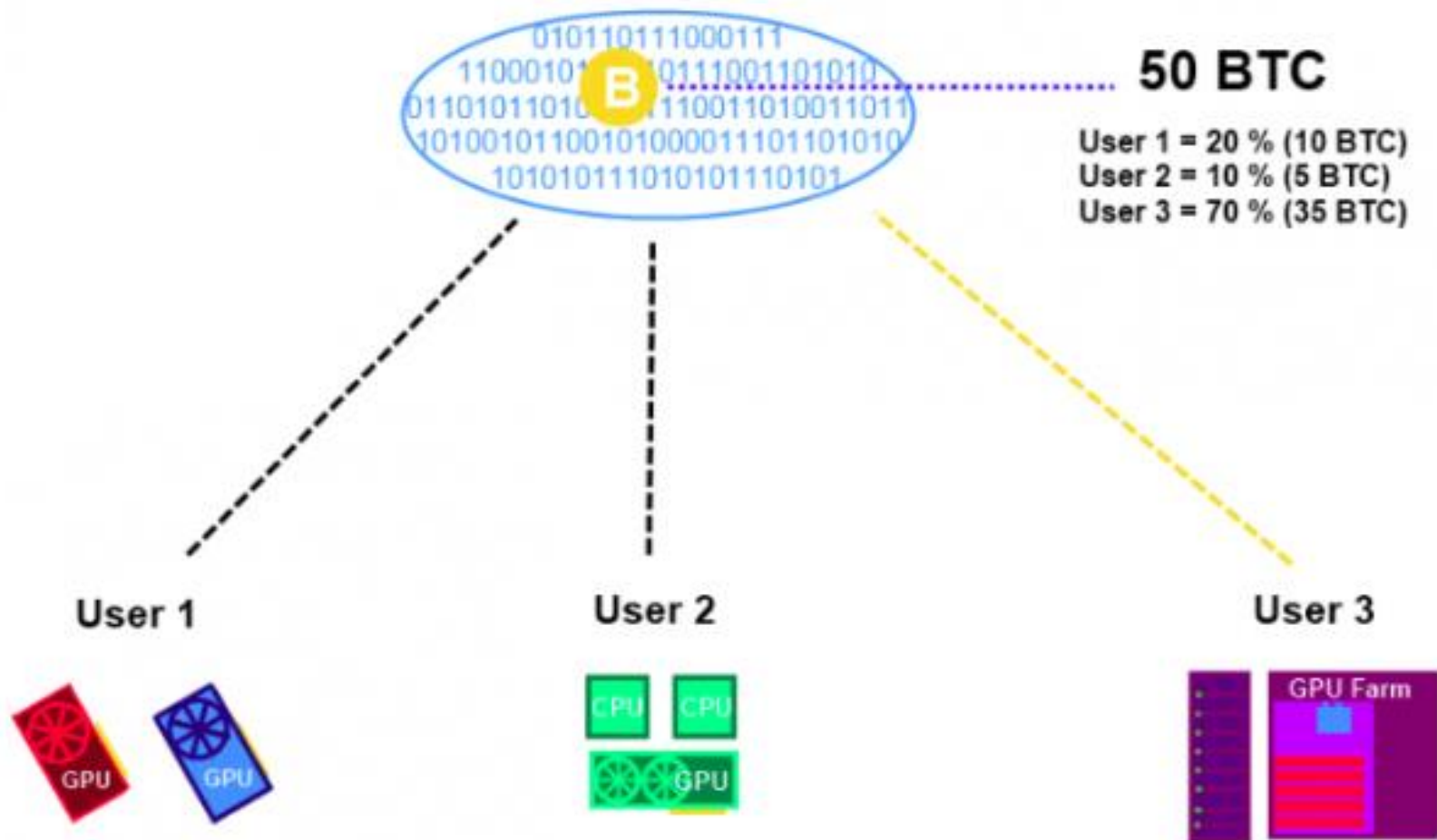
| | |
|-----------------------------------|--|
| version | 02000000 |
| previous block hash (reversed) | 17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000 |
| Merkle root (reversed) | 8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787 |
| timestamp | 358b0553 |
| bits | 535f0119 |
| nonce | 48750833 |
| transaction count | 63 |
| coinbase transaction | |
| transaction | |
| ... | |

- A transaction is created and submitted to the mining network
- A miner combines individuals transactions into a collection of transactions known as a “block”
- The miner must find a random value that when hashed with the block results in a successful hash
- The first miner to find the solution is awarded the fees

Mining complexity changes over time

- The network is designed to automatically adjust mining complexity so that a block is mined every so many minutes
- Since the goal is to be the first to mine the block, miners increase computational power to race to the finish
- The network adjusts to the new level of computational power, and those without that computational power are unable to compete

Many join pools to keep up



Mining pools payout in multiple ways

- Pay Per Share
 - Paid for the difficulty of the work done regardless of whether a block was successfully mined
 - Greatest risk for mining pool coordinators
 - Lower rate of payout
 - Your Raspberry Pi, iPhone 7, and even your Commodore 64 could result in a payout
- Proportional
 - Paid for the difficulty of the work done if the pool found a valid block
 - Greatest risk for mining pool participates
 - Higher rate of payout
- Hybrid

Miners borrow your processing power

Cryptocurrency Mining Malware Infected Over Half-Million PCs Using NSA Exploit

Wednesday, January 31, 2018 Swati Khandelwal

Share Share Tweet Share Share Find Share



Cryptocurrency-mining malware put UK and US government machines to work

Posted Feb 12, 2018 by Taylor Hatmaker (@tayhatmaker)

- Steep startup costs make it cheaper to borrow processing power
- Weak cyber defenses leave you vulnerable

Persistent Mining Software

- Requires an exploit to become persistent on the host
- Once exploited, mining software is downloaded and run on host
 - Exploit utilizes bash, Powershell, etc to download the appropriate mining software
- Communicates with mining pool using predefined protocol and ports
- May attempt to spread to additional hosts via EternalBlue, Mimikatz, WMI
- May be bundled with additional malware

Mitigations

- Typical malware defenses
 - Keep it from getting in
 - Domain or IP blocking on perimeter
 - Patching
 - Keep it from calling home
 - Port blacklisting
 - Application blocking
 - Communication signature matching
 - Keep it from spreading
 - Binary whitelisting/blacklisting on endpoints
 - Look for it
 - Monitoring of network traffic

Browser Based Mining Software

- User visits a webpage with mining JavaScript embedded
- JavaScript may be hosted intentionally or maliciously
- JavaScript is executed with the same privileges granted to all JavaScript applications
- User is unaware mining is occurring unless they are monitoring CPU usage
- Mining ceases when user navigates away from page or closes browser

Mitigations

- Typical Adware defenses
 - Keep it from getting in
 - Domain or IP blocking on perimeter
 - Employ browser extensions
 - Disable JavaScript
 - Keep it from calling home
 - Port blacklisting
 - Application blocking
 - Communication signature matching
 - Keep it from spreading
 - Look for it
 - Javascript Detection



Making cybersecurity local, personal, and actionable

Introducing MITRE and the Regional Virginia Information Sharing and Analysis Organization (VA-ISA0)

**Presentation to Virginia Information Security Officers Advisory Group
Meeting**

Gabe Galvan, Executive Director, MITRE Corporation

Wednesday, March 7, 2018

Working Across the Whole of Government



**Objective
Insight**

**Unique
Vantage
Point**

**Deep
Technical
Know-How**

**Mission
Driven**

**Pioneering together to bring innovative ideas into
existence**

MITRE Was Established to Serve the Public Interest

established
1958

**not-for-
profit**

**conflict-
environment
free**

science &
technology



**Part of the ecosystem of federal
research centers**

Solving Problems for a Safer World



Cyber @ MITRE

National Cybersecurity FFRDC: A Collaborative Hub for Cybersecurity

| 24 |

**communi-
ties of
interest**
identify and
shape
challenges

**commerc-
ially
available
products**
for example
solutions

**engagem-
ent** with
industry,
government,
and academia

to drive
technology
development



**NCF powers the National Cybersecurity
Center of Excellence (NCCoE) for NIST**

Focus Areas



Build Resilience



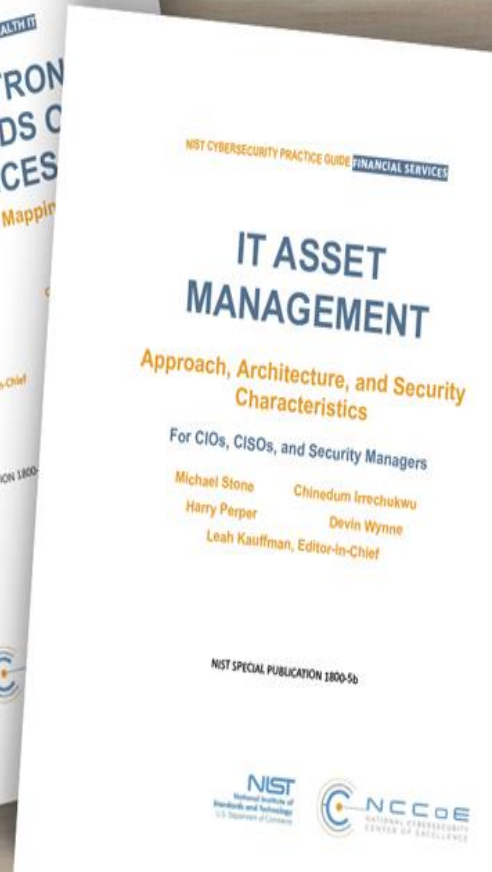
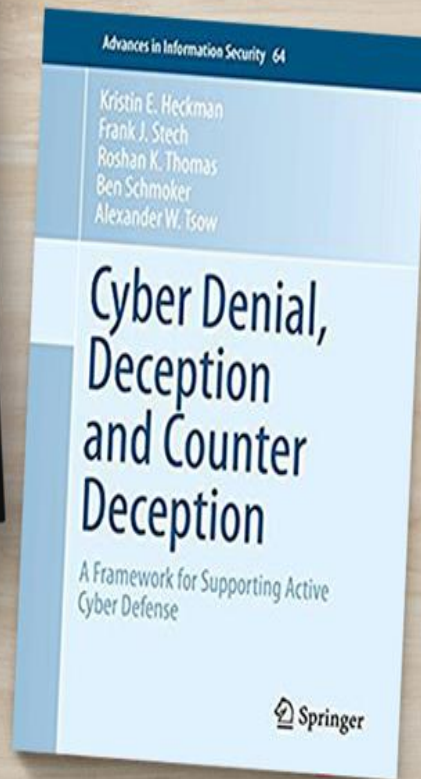
Secure Network Infrastructure



Cyber-Physical Security



Expand Community-based Analytic Sharing



Experiences with various organizations collaborating regions and industry



Cybersecurity Information Sharing History

Presidential Directive 63 (1998)

Public and private sectors must share information about physical and cyber threats/vulnerabilities to help protect the critical infrastructures

1999 Financial Services-Information Sharing and Analysis Center (FS-ISAC), followed by other ISACs

Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing (Feb 2015)

“ISAOs [Information Sharing and Analysis Organizations] may be organized on the basis of sector, sub-sector, region, or any other affinity... ISAO membership may be drawn from the public or private sectors...”

ISAO Standards Organization stood up with funding from DHS at the end of Oct 2015: “To improve the Nation’s cybersecurity posture by identifying standards and guidelines for... information

VA-ISA0 Creation

On April 20, 2015, Gov. McAuliffe announced nation's first state-level ISA0

Regional

Supports public and private cross-sector organizations

Secretary Jackson:
“Leverage our existing and future information sharing efforts”

Seed funding allocated for FY17 and FY18

The MITRE Corporation tasked with standing up the VA-ISA0

Office of Technology leadership with CIT Oversight

How can we flip the economics of attacks?

Survey of 300+ “threat experts”

- Cost of hacking is decreasing
- Threat intelligence sharing is best defense
 - Number 1 out of 21 defensive options

Sharing Reality

- Only 33% of organizations say they are satisfied with sharing efforts ⁽⁷⁾
- 27% of respondents believe their organizations are “very effective” in utilizing threat data ⁽⁸⁾

Making Information Sharing Work in the Real World: Hub & Spoke Model

Model

Technology

Infrastructure

Data Repository

Sharing Services

Cyber Testbed

Benefits

Shared technology infrastructure

Richer database

Shared cyber analytic resources

Reduces stand up time and cost per CCC

Supports sustainment

Mid-Atlantic Cyber Center

Powered by
The MITRE Corporation

Virginia ISAO
NoVa Cyber Collaboration Center (CCC)

Richmond CCC

Where Next?

Mid-Atlantic Cyber Center (MACC)

Next generation of ISAOs

Leverages MITRE's neutral, trusted, non-profit role to provide organizations in the mid-Atlantic with access to MITRE's expertise and ongoing research & development in cybersecurity and technology

Enables organizations at any stage of cybersecurity maturity to take advantage of information/threat sharing model, using tailored guidance supported by a technology infrastructure that facilitates coordinated, trusted sharing

Allows partners to benefit from economies of scale,

VA-ISA0: Regional Collaboration for Broader Impact

Fosters information sharing among Virginia's public and private sector stakeholders to improve cyber defense and mitigate associated risks

Establishes Cyber Collaboration Centers (CCCs) across the Commonwealth, organized around location and affinities among members, such as size, supply chain, or cyber ability

CCCs enable faster detection and coordinated response through local peer-to-peer sharing

What Do VA-ISA0 Members Receive?

| | Founding Member | Base Member | VA State Agencies |
|---|-----------------|-------------|-------------------|
| Governance board membership | ✓ | | ✓ |
| Base membership for supply chain vendors | ✓ | | ✓ |
| Quarterly CISO Summits | ✓ | ✓ | ✓ |
| Personalized cyber profile generated from a Cyber Operations Rapid Assessment (CORA) | ✓ | ✓ | ✓ |
| Independent log file review for adversary activity | ✓ | ✓ | ✓ |
| Cyber workshops tailored to member needs | ✓ | ✓ | ✓ |
| Curated cyber information via a private portal site | ✓ | ✓ | ✓ |
| Face-to-face and automated confidential cyber collaboration | ✓ | ✓ | ✓ |
| Cyber test bed and technology infrastructure provided by the Mid-Atlantic Cyber Center (MACC) | ✓ | ✓ | ✓ |
| Timely, relevant threat information from dedicated cyber analysts | ✓ | ✓ | ✓ |
| Advanced threat analytics sharing through ATT&CK community | ✓ | ✓ | ✓ |

Testimonial

“

Until this pilot, I didn't know there was a cyber sharing organization for my services-focused company. In confidential sessions with other pilot participants, I met other regional cyber leaders and learned about different cyber operational approaches (including primary drivers and pitfalls) which I used to inform and shape my company's cyber strategy. Beyond that, the pilot was structured so that I had the opportunity to address my questions both in a group and/or one-on-one formats.

Why Join the VA-ISA0?

**Strengthen your
cyber defense
posture**

**Elevate your
workforce
through
community**

**Be positioned to
assimilate and share
timely information
for your defense**

**Mitigate risk to
your business
operation**

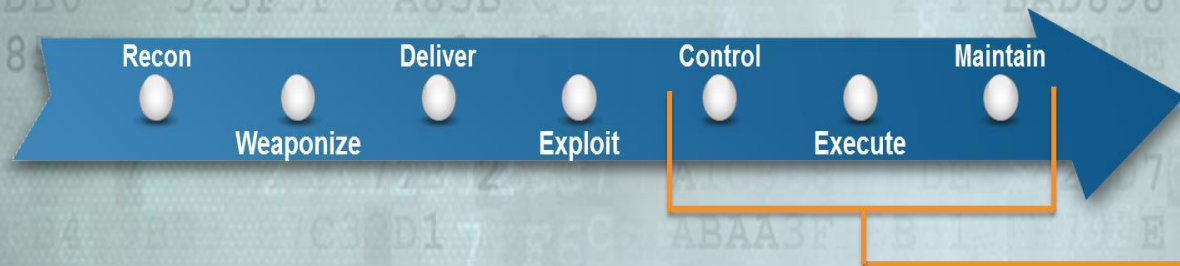
**Offload
costs**

Back- up

If I understood my adversary, I could...

- Perform gap analysis of my current defenses
- Prioritize detection/mitigation of heavily used techniques
- Track a specific adversary's set of techniques
- Conduct adversary emulation (e.g. red-teaming)
- Better evaluate new security technologies

ATT&CK: Deconstructing the Lifecycle



- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

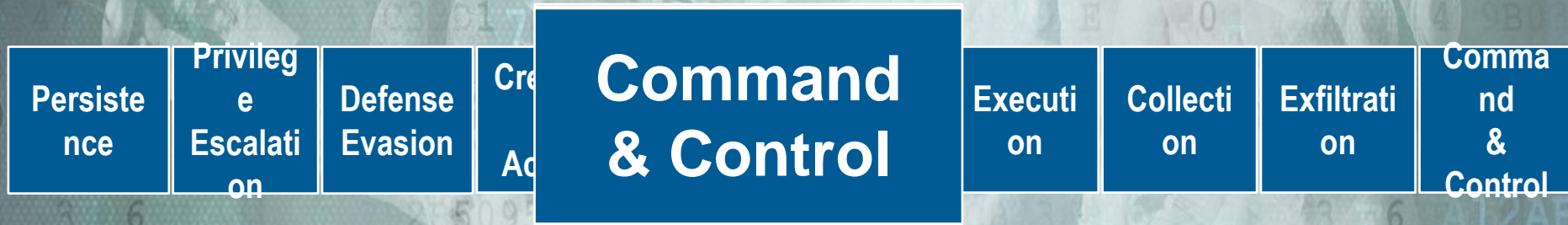
Freely available, curated knowledge base of observed adversary behavior

Higher fidelity on right-of-exploit, post-access phases

Describes behavior sans adversary tools

Working with world-class researchers to

ATT&CK Matrix: *Tactics & Techniques*



Tactic: Technical goal of the adversary

| DLL Search Order Hijacking | | Brute Force | Account Discovery | Windows Remote Management | | Audio Capture | Automated Exfiltration | Commonly Used Port | |
|---|-----------------------------|--|---------------------------------------|---------------------------------|-------------------------------|------------------------------------|---|---------------------------------------|---|
| Legitimate Credentials | | Credential Dumping | Application Window Discovery | Third-party Software | | Automated Collection | Data Compressed | Communication Through Removable Media | |
| Accessibility Features | Binary Padding | | | Application Deployment Software | Command-Line | Clipboard Data | Data Encrypted | Connection Proxy | |
| Applnit DLLs | Code Signing | Credential Manipulation | File and Directory Discovery | Exploitation of Vulnerability | Execution through API | Data Staged | Data Transfer Size Limits | | Custom Command and Control Protocol |
| Local Port Monitor | Component Firmware | | | | Execution through Module Load | Data from Local System | Exfiltration Over Alternative Protocol | | |
| New Service | DLL Side-Loading | Credentials in Files | Local Network Configuration Discovery | Logon Scripts | Graphical User Interface | Data from Network Shared Drive | Exfiltration Over Command and Control Channel | Custom Cryptographic Protocol | |
| Path Interception | Disabling Security Tools | Input Capture | Local Network Connections Discovery | Pass the Hash | InstallUtil | Data from Removable Media | | | |
| Scheduled Task | File Deletion | Network Sniffing | | Pass the Ticket | MSBuild | Email Collection | Exfiltration Over Other Network Medium | Data Encoding | |
| File System Permissions Weakness | File System Logical Offsets | Two-Factor Authentication Interception | Remote Desktop Protocol | PowerShell | | | | | |
| Service Registry Permissions Weakness | | | | Remote File Copy | Process Hollowing | Input Capture | | | |
| Web Shell | Indicator Blocking | | | | | | | Callback Channels | |
| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command & Control |
| Basic Input/Output System | | Indicator Removal from Tools | | Remote System Discovery | Windows Admin Shares | Service Execution | | | Standard Application Layer Protocol |
| Change Default File Association | | Indicator Removal on Host | | Security Software Discovery | | Windows Management Instrumentation | | | Standard Cryptographic Protocol |
| Component Firmware | | Install Root Certificate | | System Information Discovery | | | | | Standard Non-Application Layer Protocol |
| External Remote Services | | InstallUtil | | | | | | | |
| Hypervisor | | Masquerading | | System Owner/User Discovery | | | | | Uncommonly Used Port |
| Logon Scripts | | Modify Registry | | System Service Discovery | | | | | Web Service |
| Modify Existing Service | | MSBuild | | System Time Discovery | | | | | |
| Netsh Helper DLL | | Network Share Removal | | | | | | | |
| Redundant Access | | NTFS Extended Attributes | | | | | | | |
| Registry Run Keys / Start Folder | | Obfuscated Files or Information | | | | | | | |
| Security Support Provider | | Process Hollowing | | | | | | | |
| Shortcut Modification | | Redundant Access | | | | | | | |
| Windows Management Instrumentation Event Subscription | | Regsvcs/Regasm | | | | | | | |
| Winlogon Helper DLL | | Regsvr32 | | | | | | | |
| | | Rootkit | | | | | | | |
| | | Rundll32 | | | | | | | |
| | | Scripting | | | | | | | |
| | | Software Packing | | | | | | | |
| | | Timestamp | | | | | | | |

Technique: How adversary achieves the goal

Technique: How adversary achieves the goal

Example Tactic: Persistence

Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.

Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.

Example Technique: New Service

- **Description:** When operating systems boot up, they can start programs or applications called services that perform background system functions. Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools.
- **Platform:** Windows
- **Permissions required:** Administrator, SYSTEM
- **Effective permissions:** SYSTEM
- **Detection**
 - Monitor service creation through changes in the Registry and common utilities using command-line invocation
 - Tools such as Sysinternals Autoruns may be used to detect system changes that could be attempts at persistence
 - Monitor processes and command-line arguments for actions that could create services
- **Mitigation**
 - Limit privileges of user accounts and remediate Privilege Escalation vectors
 - Identify and block unnecessary system utilities or potentially malicious software that may be used to create services
- **Data Sources:** Windows Registry, process monitoring, command-line parameters
- **Examples:** *Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, ...*
- **CAPEC ID:** CAPEC-550



Where does ATT&CK come from?

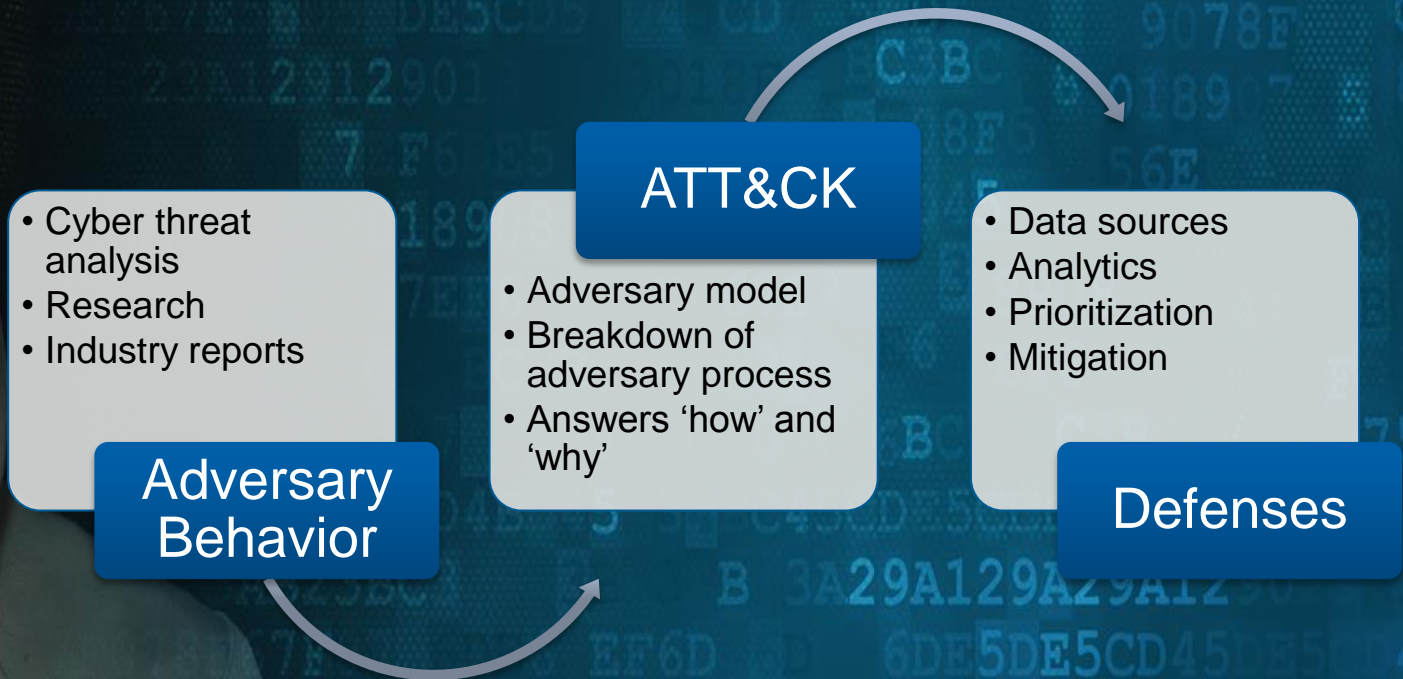
Our Living Lab – The Fort Meade Experiment (FMX)



MITRE's Annapolis Junction, MD site

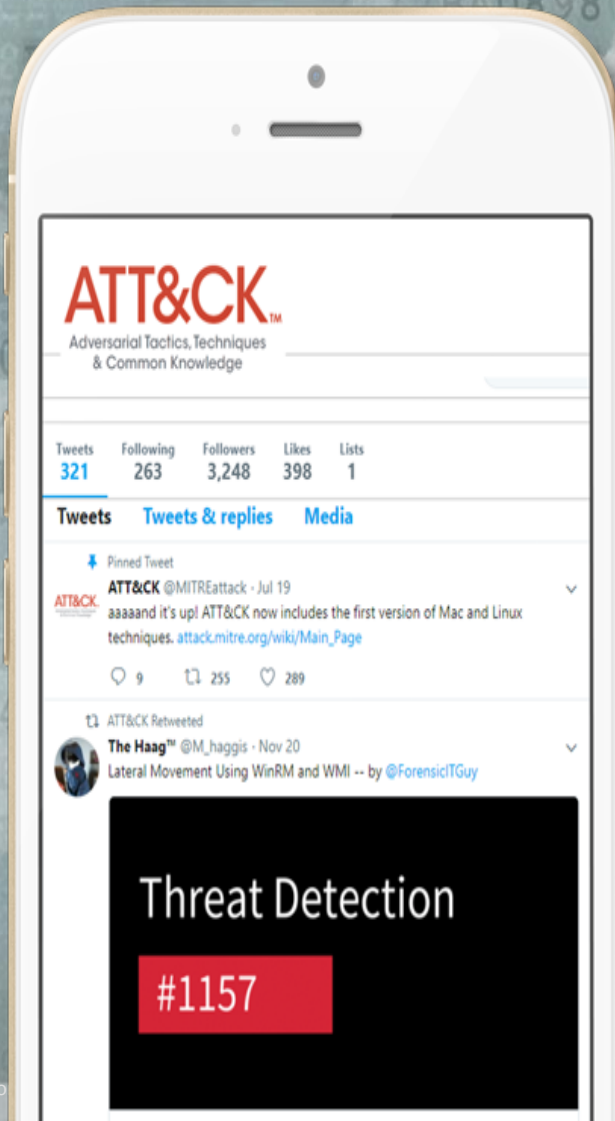
- Approx. 250 unclassified computers
- Primarily user desktops running Windows

ATT&CK's Threat-based Modeling



Who's using ATT&CK?

- End-users
- Security vendors
- Government



How do I use ATT&CK?

- Resource for threat modeling
- Red-team/blue-team planning
- Enhance threat intelligence
- Defensive planning

Example: APT 28 Reported Techniques

| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---------------------------------------|----------------------------------|-----------------------------|--|---------------------------------------|-------------------------------------|-----------------------------|------------------------------------|--------------------------------------|---|
| DLL Search Order Hijacking | | | Brute Force | Account Discovery | Windows Remote Management | | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Legitimate Credentials | | | Credential Dumping | Application Window Discovery | Third-party Software | | Automated Collection | Data Compressed | Communication Through Removable Media |
| Accessibility Features | | Binary Padding | | | Application Deployment Software | Command-Line | Clipboard Data | Data Encrypted | |
| Applnit DLLs | | Code Signing | Credential Manipulation | File and Directory Discovery | | Execution through API | Data Staged | Data Transfer Size Limits | Connection Proxy |
| Local Port Monitor | | Component Firmware | | | Exploitation of Vulnerability | | Execution through Module Load | Data from Local System | Exfiltration Over Alternative Protocol |
| New Service | | DLL Side-Loading | Credentials in Files | Local Network Configuration Discovery | | Graphical User Interface | | Data from Network Shared Drive | Exfiltration Over Command and Control Channel |
| Path Interception | | Disabling Security Tools | Input Capture | Logon Scripts | InstallUtil | | Data from Removable Media | Data Encoding | |
| Scheduled Task | | File Deletion | Network Sniffing | Local Network Connections Discovery | Pass the Hash | Email Collection | | | Exfiltration Over Other Network Medium |
| File System Permissions Weakness | | File System Logical Offsets | Two-Factor Authentication Interception | Network Service Scanning | Pass the Ticket | | MSBuild | Exfiltration Over Physical Medium | |
| Service Registry Permissions Weakness | | | | Indicator Blocking | Peripheral Device Discovery | Remote Desktop Protocol | PowerShell | | Input Capture |
| Authentication Package | Exploitation of Vulnerability | | | Permission Groups Discovery | Remote File Copy | Process Hollowing | Screen Capture | Exfiltration Over Scheduled Transfer | Multi-Stage Channels |
| | Bypass User Account Control | | | | Remote Services | Regsvcs/Regasm | | | |
| Bootkit | DLL Injection | | | Process Discovery | Replication Through Removable Media | Regsvr32 | Scheduled Task | Scripting | Multiband Communication |
| Component Object Model Hijacking | Component Object Model Hijacking | | | | Rundll32 | Service Execution | | | |
| Basic Input/Output System | Indicator Removal from Tools | | | Query Registry | Taint Shared Content | | Windows Management Instrumentation | Windows Admin Shares | Service Execution |
| Change Default File Association | Indicator Removal on Host | | | Remote System Discovery | Security Software Discovery | | | | |
| Component Firmware | Install Root Certificate | | | System Information Discovery | | System Owner/User Discovery | | | |
| External Remote Services | InstallUtil | | | | System Service Discovery | | System Time Discovery | | |
| Hypervisor | Masquerading | | | System Time Discovery | | System Time Discovery | | | |
| Logon Scripts | Modify Registry | | | | System Time Discovery | | System Time Discovery | | |
| Modify Existing Service | MSBuild | | | System Time Discovery | | System Time Discovery | | | |
| Netsh Helper DLL | Network Share Removal | | | | System Time Discovery | | System Time Discovery | | |
| Redundant Access | NTFS Extended Attributes | | | System Time Discovery | | System Time Discovery | | | |
| Registry Run Keys / Start Folder | Obfuscated Files or Information | | | | System Time Discovery | | System Time Discovery | | |
| Security Support Provider | Process Hollowing | | | System Time Discovery | | System Time Discovery | | | |
| Shortcut Modification | Redundant Access | | | | System Time Discovery | | System Time Discovery | | |
| Windows Management Instrumentation | Regsvcs/Regasm | | | System Time Discovery | | System Time Discovery | | | |
| | Regsvr32 | | | | System Time Discovery | | System Time Discovery | | |

Legend

APT 28

MIT

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Legend APT 28

Example: Comparing Groups APT 28 vs. Deep Panda

| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---------------------------------------|----------------------------------|-----------------------------|--|---------------------------------------|---------------------------------|------------------------------------|---|--------------------------------|---|
| DLL Search Order Hijacking | | | Brute Force | Account Discovery | Windows Remote Management | | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Legitimate Credentials | | | Credential Dumping | Application Window Discovery | Third-party Software | | Automated Collection | Data Compressed | Communication Through Removable Media |
| Accessibility Features | | Binary Padding | | | Application Deployment Software | Command-Line | Clipboard Data | Data Encrypted | |
| AppInit DLLs | | Code Signing | Credential Manipulation | File and Directory Discovery | | Execution through API | Data Staged | Data Transfer Size Limits | Connection Proxy |
| Local Port Monitor | | Component Firmware | | | Exploitation of Vulnerability | | Execution through Module Load | Data from Local System | Exfiltration Over Alternative Protocol |
| New Service | | DLL Side-Loading | Credentials in Files | Local Network Configuration Discovery | | Graphical User Interface | | Data from Network Shared Drive | Exfiltration Over Command and Control Channel |
| Path Interception | | Disabling Security Tools | Input Capture | | Logon Scripts | | InstallUtil | Data from Removable Media | |
| Scheduled Task | | File Deletion | Network Sniffing | Local Network Connections Discovery | Pass the Hash | Data from Removable Media | Exfiltration Over Other Network Medium | Data Obfuscation | |
| File System Permissions Weakness | | File System Logical Offsets | Two-Factor Authentication Interception | Pass the Ticket | MSBuild | | | | |
| Service Registry Permissions Weakness | | | | | Network Service Scanning | Remote Desktop Protocol | PowerShell | Email Collection | Exfiltration Over Physical Medium |
| Web Shell | | Indicator Blocking | Peripheral Device Discovery | Remote File Copy | Process Hollowing | Input Capture | Scheduled Transfer | Fallback Channels | |
| Authentication Package | Exploitation of Vulnerability | | | Remote Services | Regsvcs/Regasm | Screen Capture | | Multiband Communication | |
| | Bypass User Account Control | | | Replication Through Removable Media | Regsvr32 | Video Capture | | | |
| Bootkit | DLL Injection | | | Rundll32 | | | | | |
| Component Object Model Hijacking | Component Object Model Hijacking | | | Process Discovery | Shared Webroot | Scheduled Task | Multilayer Encryption | | |
| Basic Input/Output System | Indicator Removal from Tools | | | Query Registry | Taint Shared Content | Scripting | Remote File Copy | | |
| | | | | Remote System Discovery | Windows Admin Shares | Service Execution | Standard Application Layer Protocol | | |
| Change Default File Association | Indicator Removal on Host | | | Security Software Discovery | | Windows Management Instrumentation | Standard Cryptographic Protocol | | |
| Component Firmware | Install Root Certificate | | | System Information Discovery | | | Standard Non-Application Layer Protocol | | |
| External Remote Services | InstallUtil | | | | | | | | |
| Hypervisor | Masquerading | | | System Owner/User Discovery | | | Uncommonly Used Port | | |
| Logon Scripts | Modify Registry | | | | | | | | |
| Modify Existing Service | MSBuild | | | System Service Discovery | | | Web Service | | |
| Netsh Helper DLL | Network Share Removal | | | | | | | | |
| Redundant Access | NTFS Extended Attributes | | | System Time Discovery | | | | | |
| Registry Run Keys / Start Folder | Obfuscated Files or Information | | | | | | | | |
| Security Support Provider | Process Hollowing | | | | | | | | |
| Shortcut Modification | Redundant Access | | | | | | | | |
| Windows Management Instrumentation | Regsvcs/Regasm | | | | | | | | |
| | Regsvr32 | | | | | | | | |

Legend

APT 28
Deep
Panda

MIT

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Legend

APT 28

Deep Panda

Example: Notional Defense Gaps

| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---------------------------------------|---------------------------------|--|------------------------------|-------------------------------------|--------------------------------|---|--|---|---------------------------------------|
| DLL Search Order Hijacking | | | Brute Force | Account Discovery | Windows Remote Management | | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Legitimate Credentials | | | Credential Dumping | Application Window Discovery | Third-party Software | | Automated Collection | Data Compressed | Communication Through Removable Media |
| Accessibility Features | Binary Padding | Application Deployment Software | | Command-Line Execution through API | Clipboard Data | Data Encrypted | Connection Proxy | | |
| AppInit DLLs | Code Signing | | File and Directory Discovery | | Execution through Module Load | Data Staged | Data Transfer Size Limits | Connection Proxy | |
| Local Port Monitor | Component Firmware | Exploitation of Vulnerability | | Graphical User Interface | | Data from Local System | Exfiltration Over Alternative Protocol | Custom Command and Control Protocol | |
| New Service | DLL Side-Loading | | Logon Scripts | | Data from Network Shared Drive | Exfiltration Over Command and Control Channel | Custom Cryptographic Protocol | | |
| Path Interception | Disabling Security Tools | Pass the Hash | | InstallUtil | | | | | |
| Scheduled Task | File Deletion | Network Sniffing | Pass the Ticket | MSBuild | Data from Removable Media | Data Encoding | | | |
| File System Permissions Weakness | File System Logical Offsets | Two-Factor Authentication Interception | Network Service Scanning | Remote Desktop Protocol | PowerShell | Email Collection | Exfiltration Over Other Network Medium | Data Obfuscation | |
| Service Registry Permissions Weakness | | | Peripheral Device Discovery | Remote File Copy | Process Hollowing | Input Capture | Exfiltration Over Physical Medium | Fallback Channels | |
| Web Shell | | Indicator Blocking | Permission Groups Discovery | Remote Services | Regsvcs/Regasm | Screen Capture | Exfiltration Over Physical Medium | Multi-Stage Channels | |
| Authentication Package | Exploitation of Vulnerability | | | Replication Through Removable Media | Regsvr32 | Video Capture | Scheduled Transfer | Multiband Communication | |
| Bootkit | Bypass User Account Control | | | Shared Webroot | Scheduled Task | | | Multilayer Encryption | |
| Component Object Model Hijacking | DLL Injection | | | Query Registry | Taint Shared Content | Scripting | | Remote File Copy | |
| Basic Input/Output System | Indicator Removal from Tools | | | Remote System Discovery | Windows Admin Shares | Service Execution | | Standard Application Layer Protocol | |
| Change Default File Association | Indicator Removal on Host | | | Security Software Discovery | | Windows Management Instrumentation | | Standard Cryptographic Protocol | |
| Component Firmware | Install Root Certificate | | | System Information Discovery | | | | Standard Non-Application Layer Protocol | |
| External Remote Services | InstallUtil | | | | | | | | |
| Hypervisor | Masquerading | | | System Owner/User Discovery | | | | | |
| Logon Scripts | Modify Registry | | | System Service Discovery | | | | | |
| Modify Existing Service | MSBuild | | | System Time Discovery | | | | | |
| Netsh Helper DLL | Network Share Removal | | | | | | | | |
| Redundant Access | NTFS Extended Attributes | | | | | | | | |
| Registry Run Keys / Start Folder | Obfuscated Files or Information | | | | | | | | |
| Security Support Provider | Process Hollowing | | | | | | | | |
| Shortcut Modification | Redundant Access | | | | | | | | |
| Windows Management Instrumentation | Regsvcs/Regasm | | | | | | | | |
| | Regsvr32 | | | | | | | | |

MITRE

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Example: Adversary Visibility at the Perimeter

| Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Execution | Collection | Exfiltration | Command and Control |
|---------------------------------------|-------------------------------|----------------------------------|--|-------------------------------------|-------------------------------|------------------------------------|-------------------------------------|---|---------------------------------------|
| DLL Search Order Hijacking | | | Brute Force | Account Discovery | Windows Remote Management | | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Legitimate Credentials | | | Credential Dumping | Application Window Discovery | Third-party Software | | Automated Collection | Data Compressed | Communication Through Removable Media |
| Accessibility Features | | Binary Padding | | Application Deployment Software | Command-Line | Clipboard Data | Data Encrypted | Connection Proxy | |
| Appinit DLLs | | Code Signing | File and Directory Discovery | | Execution through API | Data Staged | Data Transfer Size Limits | | |
| Local Port Monitor | | Component Firmware | Credential Manipulation | File and Directory Discovery | Exploitation of Vulnerability | Execution through Module Load | Data from Local System | Exfiltration Over Alternative Protocol | Custom Command and Control Protocol |
| New Service | | DLL Side-Loading | | | | | Credentials in Files | Local Network Configuration Discovery | Data from Network Shared Drive |
| Path Interception | | Disabling Security Tools | Input Capture | Logon Scripts | Graphical User Interface | | | | |
| Scheduled Task | | File Deletion | Network Sniffing | Local Network Connections Discovery | Pass the Hash | InstallUtil | Data from Removable Media | Data Encoding | |
| File System Permissions Weakness | | File System Logical Offsets | Two-Factor Authentication Interception | Network Service Scanning | Pass the Ticket | MSBuild | Email Collection | | |
| Service Registry Permissions Weakness | | | | Indicator Blocking | Peripheral Device Discovery | Remote Desktop Protocol | PowerShell | Exfiltration Over Other Network Medium | Data Obfuscation |
| Web Shell | | | | Remote File Copy | Process Hollowing | Input Capture | Exfiltration Over Physical Medium | Fallback Channels | |
| Authentication Package | Exploitation of Vulnerability | | | Remote Services | Regsvcs/Regasm | Screen Capture | Scheduled Transfer | Multi-Stage Channels | |
| | Bypass User Account Control | | | Replication Through Removable Media | Regsvr32 | Video Capture | | Multiband Communication | |
| Bootkit | DLL Injection | | | | Rundll32 | | | | |
| Component Object Model Hijacking | | Component Object Model Hijacking | | Process Discovery | Shared Webroot | Scheduled Task | | Multilayer Encryption | |
| Basic Input/Output System | | Indicator Removal from Tools | | Query Registry | Taint Shared Content | Scripting | | Remote File Copy | |
| | | | Remote System Discovery | Windows Admin Shares | Service Execution | | Standard Application Layer Protocol | | |
| Change Default File Association | | Indicator Removal on Host | | Security Software Discovery | | Windows Management Instrumentation | | Standard Cryptographic Protocol | |
| Component Firmware | | Install Root Certificate | | System Information Discovery | | | | Standard Non-Application Layer Protocol | |
| External Remote Services | | InstallUtil | | | | | | | |
| Hypervisor | | Masquerading | | | | | | | |
| Logon Scripts | | Modify Registry | | | | | | | |
| Modify Existing Service | | MSBuild | | System Owner/User Discovery | | | | | |
| Netsh Helper DLL | | Network Share Removal | | System Service Discovery | | | | | |
| Redundant Access | | NTFS Extended Attributes | | System Time Discovery | | | | | |
| Registry Run Keys / Start Folder | | Obfuscated Files or Information | | | | | | | |
| Security Support Provider | | Process Hollowing | | | | | | | |
| Shortcut Modification | | Redundant Access | | | | | | | |
| Windows Management Instrumentation | | Regsvcs/Regasm | | | | | | | |
| | | Regsvr32 | | | | | | | |

MITRE

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Copyright 2018 MITRE Corporation. All rights reserved.

| | | | |
|-----------------|----------------|---------------|------|
| High Confidence | Med Confidence | No Confidence | Used |
|-----------------|----------------|---------------|------|

ATT&CK Resources

- Website: attack.mitre.org
- Email: attack@mitre.org
- Twitter: @MITREattack
- STIX 2 representations of ATT&CK knowledge base:
<https://github.com/mitre/cti>





Virginia Information Technologies Agency



Google Messaging Transition and Virtru Encryption

John Craft
Deputy CISO



Overview

- Transition Update
- Enterprise Messaging Security Classification
- Enterprise Options
- Architecture Overview
- G Suite and Virtru Security Controls



Transition update

Transition from NG-managed Microsoft Exchange to Google G Suite

- November 11, 2017 – Initial 250 CoreIT users transitioned to Google
- January 22, 2018 – Approx. 12,000 Early adopters transitioned to Google
- March 26, 2018 – Remaining users will transition to Google



Enterprise Messaging

- Messaging service has two platform utilization options:
 - Standard
 - Non-sensitive
 - Secure
 - Sensitive data
 - Agencies make risk decision to authorize transmission of sensitive data via the platform
 - Enterprise provides encryption capability through Virtru
- CSRM recommends that sensitive data not be shared through email

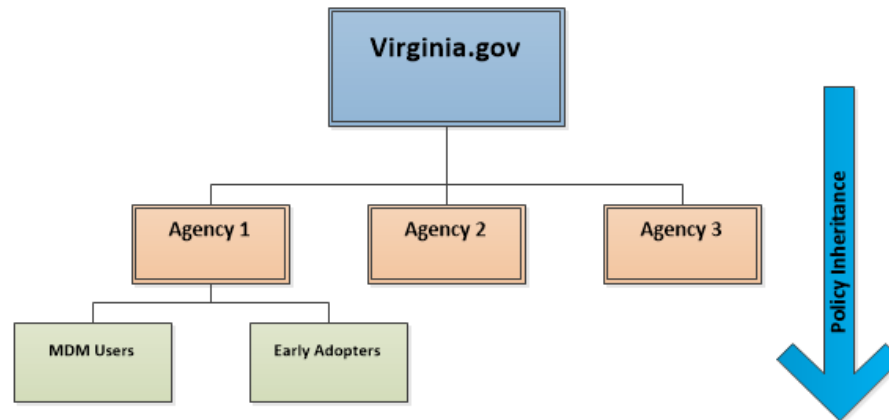


Enterprise Options

- Two Options available for agencies:
 - Basic Mailbox
 - 30Gb Storage
 - No Google Vault
 - Google Apps Unlimited
 - Unlimited storage
 - Google Vault
- Chrome is the recommended G Suite messaging client, however Outlook can be configured as well

G Suite Architecture Overview

- Structured similarly to AD:
 - Agencies are assigned to Organizational Units (OU) with Virginia.gov as the top-level domain
 - Each agency OU can have sub-OUs
 - Policies can be applied at the domain and OU levels





G Suite Standard Security Controls

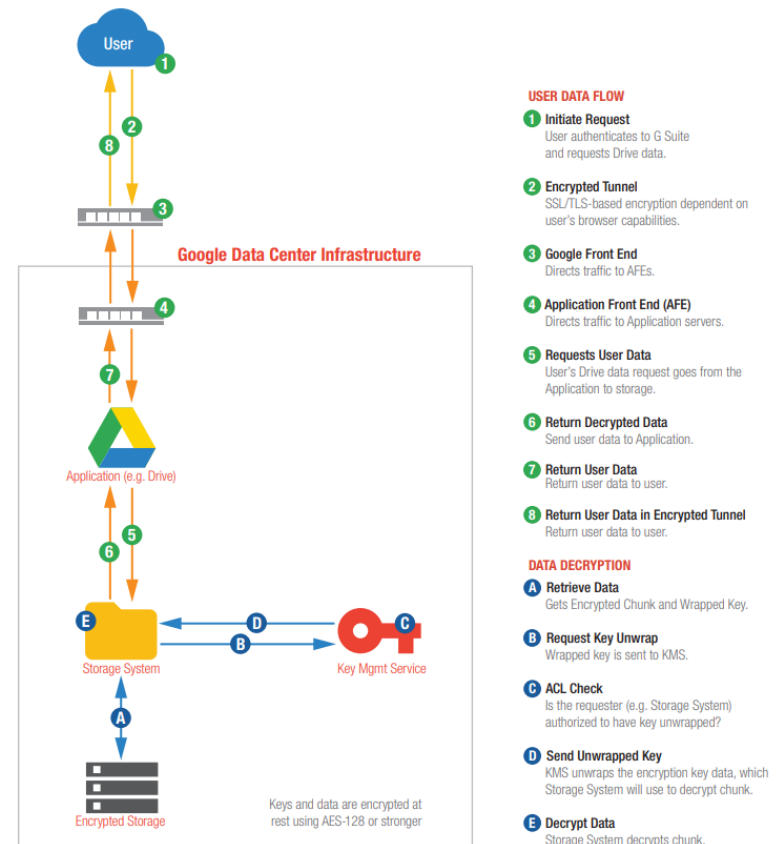
- Anti-Spam
- Anti-Malware / Phishing
- Single Sign-on
- Multi-factor Authentication (MFA)
- Message Archival (Vault)
- Security Analytics Dashboard
- Mobile Device Management (MDM)
- Data Loss Prevention (DLP)

G Suite Standard Security Controls

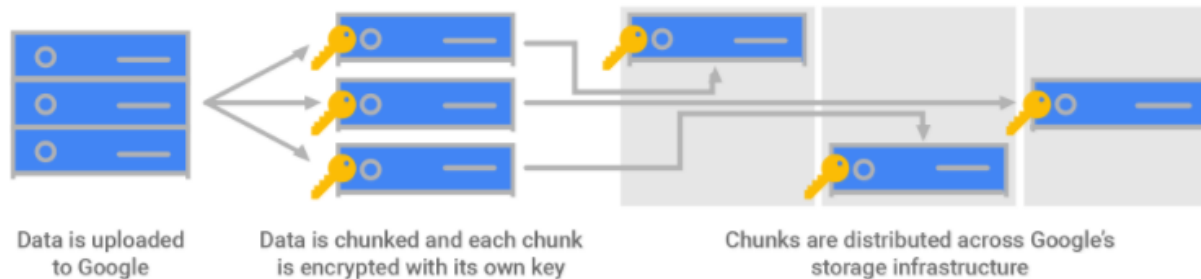
- Encryption
 - In-transit (TLS)
 - At-rest
 - Data chunks
 - Key Management server
 - Rotating keys

Encryption at Rest Flow

An example of encryption in Google Drive



Data Chunking and Encryption

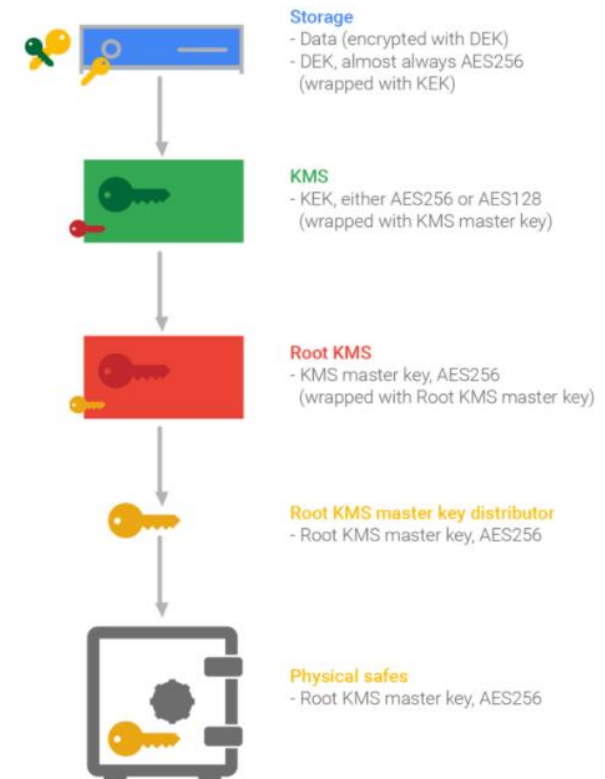


- Common cryptographic library is CrunchyCrypt, which leverages BoringSSL (Google's fork of OpenSSL)
 - Open Source
- Preferred encryption protocols for data at-rest: AES-GCM (256-bit), HMAC-SHA256



Key Management Hierarchy

- Google utilizes a key hierarchy and root of trust principle
 - Data is chunked and encrypted with DEKs
 - DEKs are encrypted with KEKs
 - KEKs are stored in KMS
 - KMS keys are wrapped with the KMS master key (stored in the Root KMS)
 - KMS master keys are wrapped with the root KMS master key (stored in the root KMS master key distributor)
 - Root KMS master key distributor is peer-to-peer, runs in RAM, and gets keying material from other running instances





G Suite Regulatory Compliance

- ISO 27001, 27017, 27018 certifications
- SOC2/3 Audits
 - Security, availability, processing integrity, and confidentiality trust principles
- PCI DSS (DLP policy)
- FedRAMP Moderate ATO
 - PII and Controlled Unclassified Information (CUI)



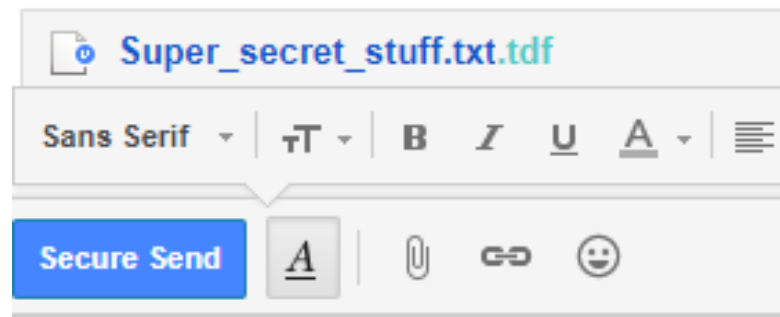
Virtu

- Works with both Google and Microsoft
 - Chrome Extension
 - Outlook Plugin
- Centralized Administrative Policies
- Granular Insight and Control
- E-Discovery Support
- Data Loss Prevention (DLP)



Virtru Basics

- Based on the Trusted Data Format (TDF)
 - Used by the U.S. intelligence community
- Encryption occurs in the client prior to transmission
- Email body and all attachments are individually encrypted using separate AES-256 bit access control keys

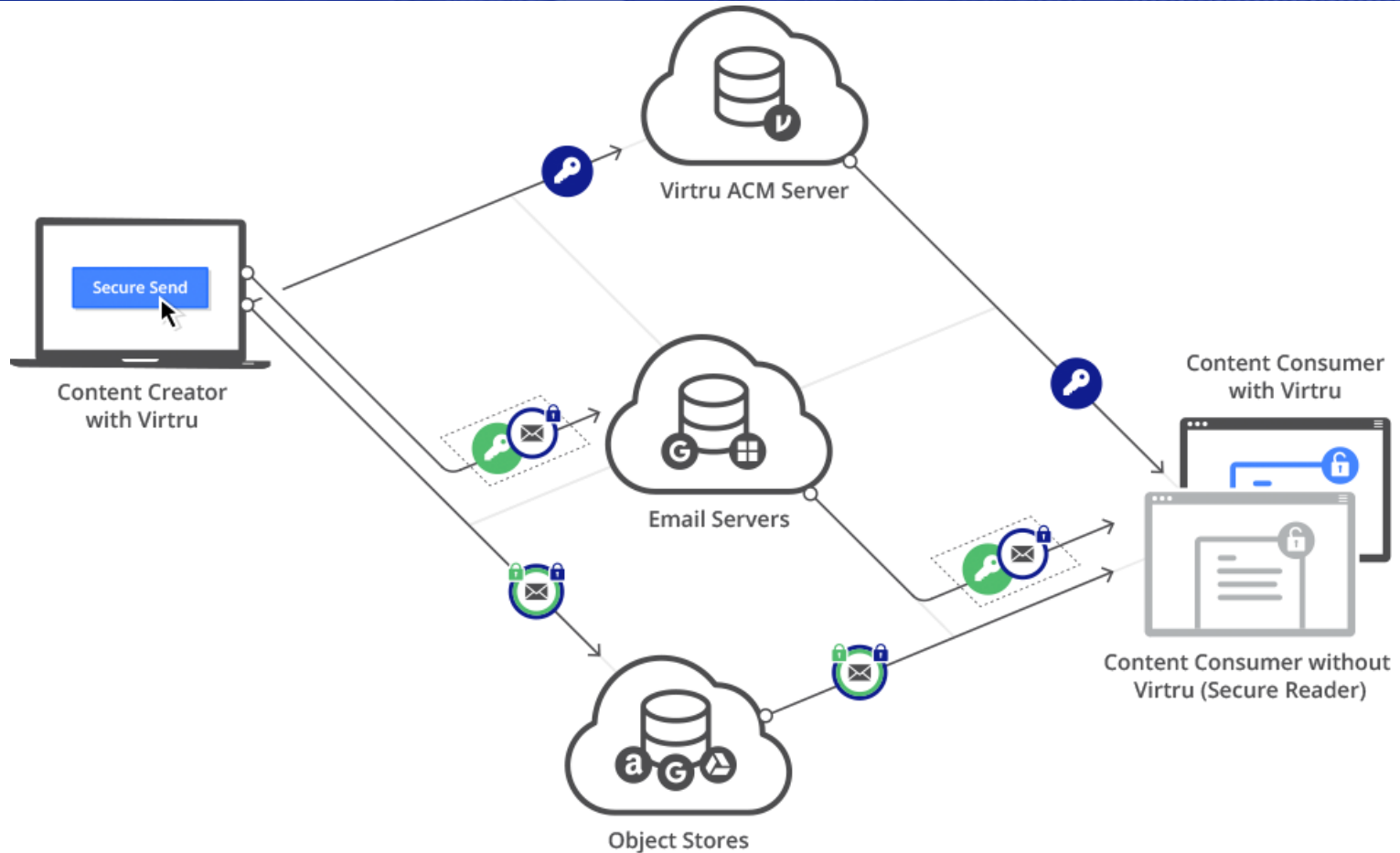


Virtru to Virtru

1. Message is encrypted in the client with access control key.
2. Key(s) uploaded to Virtru ACM with PFS (ECDHE)
3. Encrypted message sent to mail server
4. Recipient authenticates to the ACM server for access control key retrieval
5. Decrypt message with key



Virtru to non-Virtru

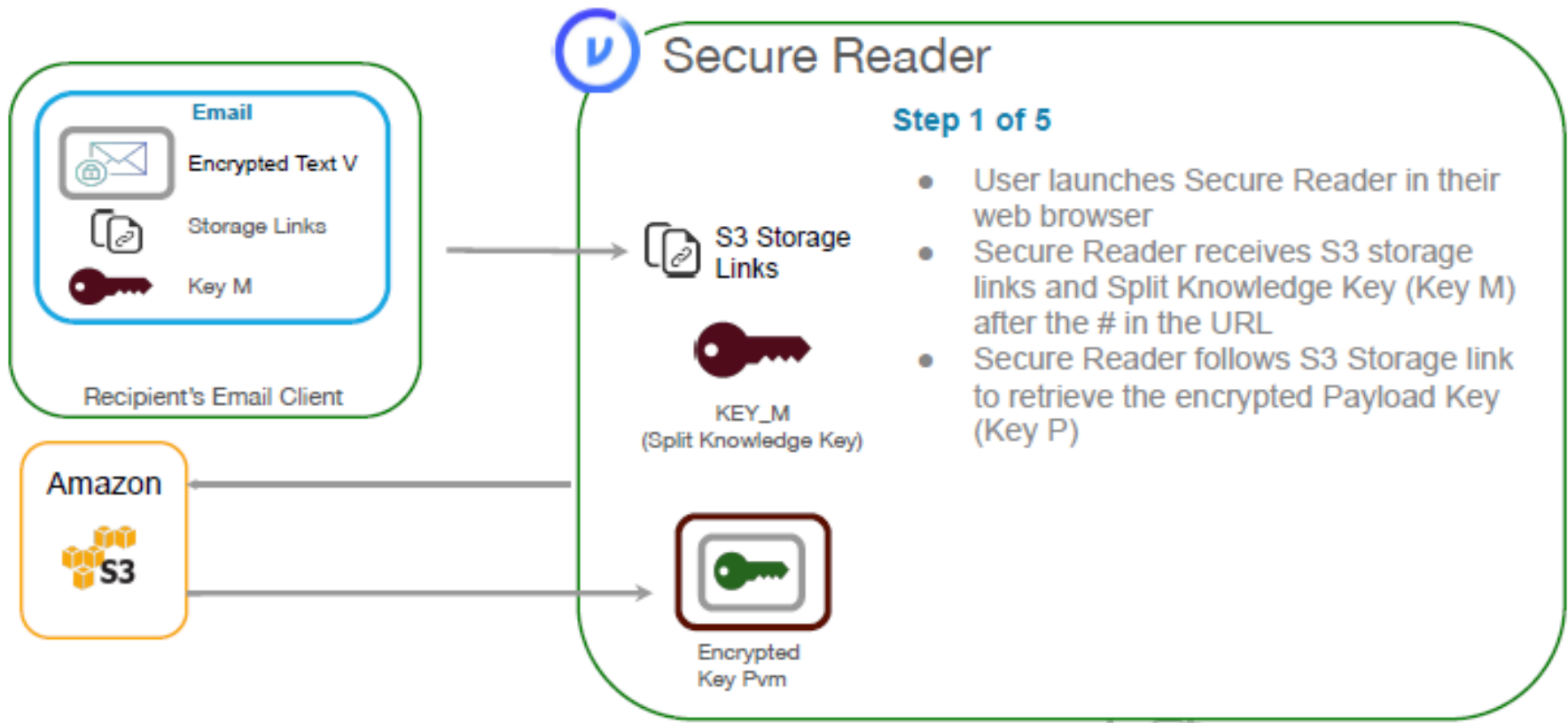




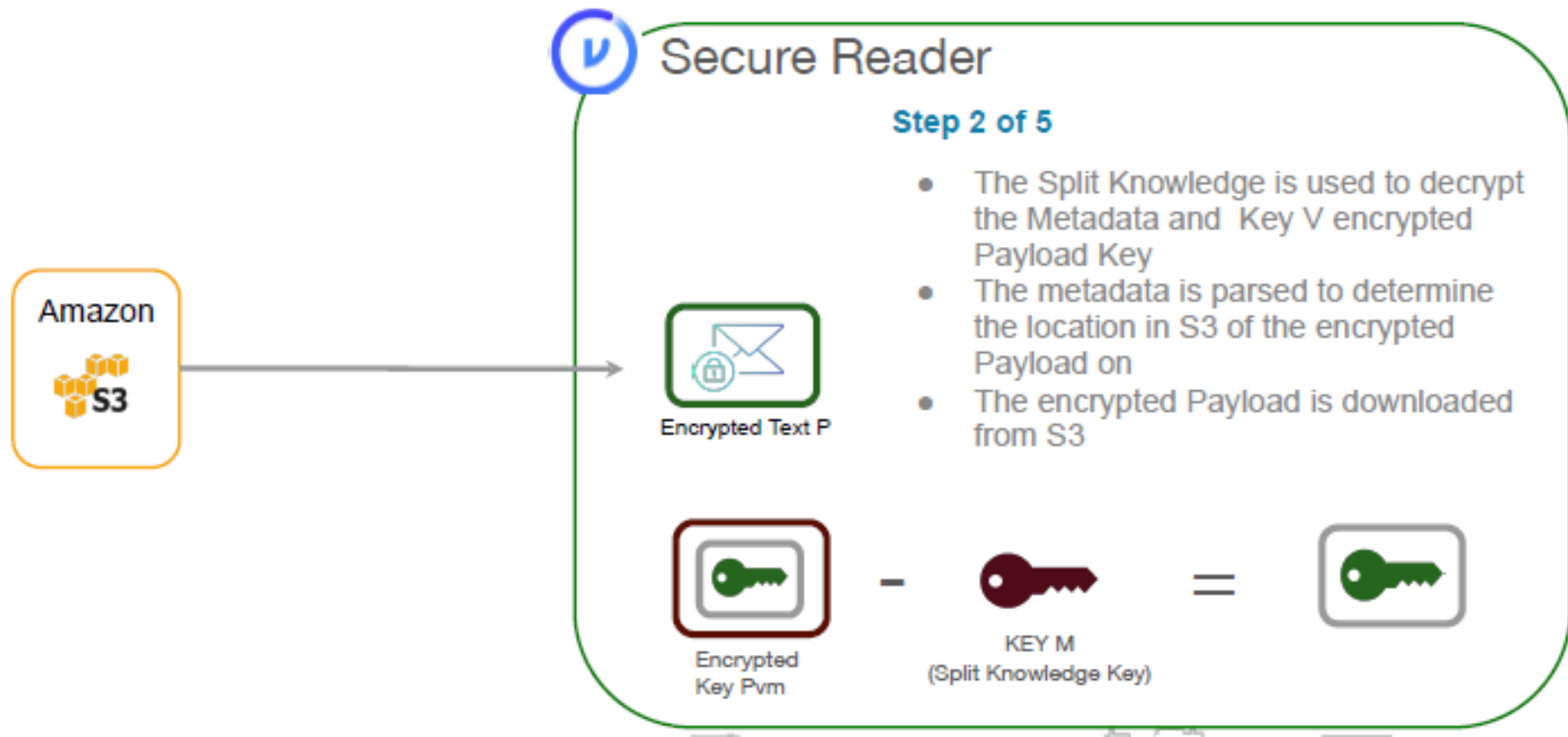
Virtru to non-Virtru

- Secure Reader
- Leverages fragment identifiers and split knowledge keys
 - Fragment identifiers identifies something specific about a document and is not seen by the server
 - <http://www.example.org/foo.html#bar>
- Split knowledge key and storage links are transmitted as fragment identifiers

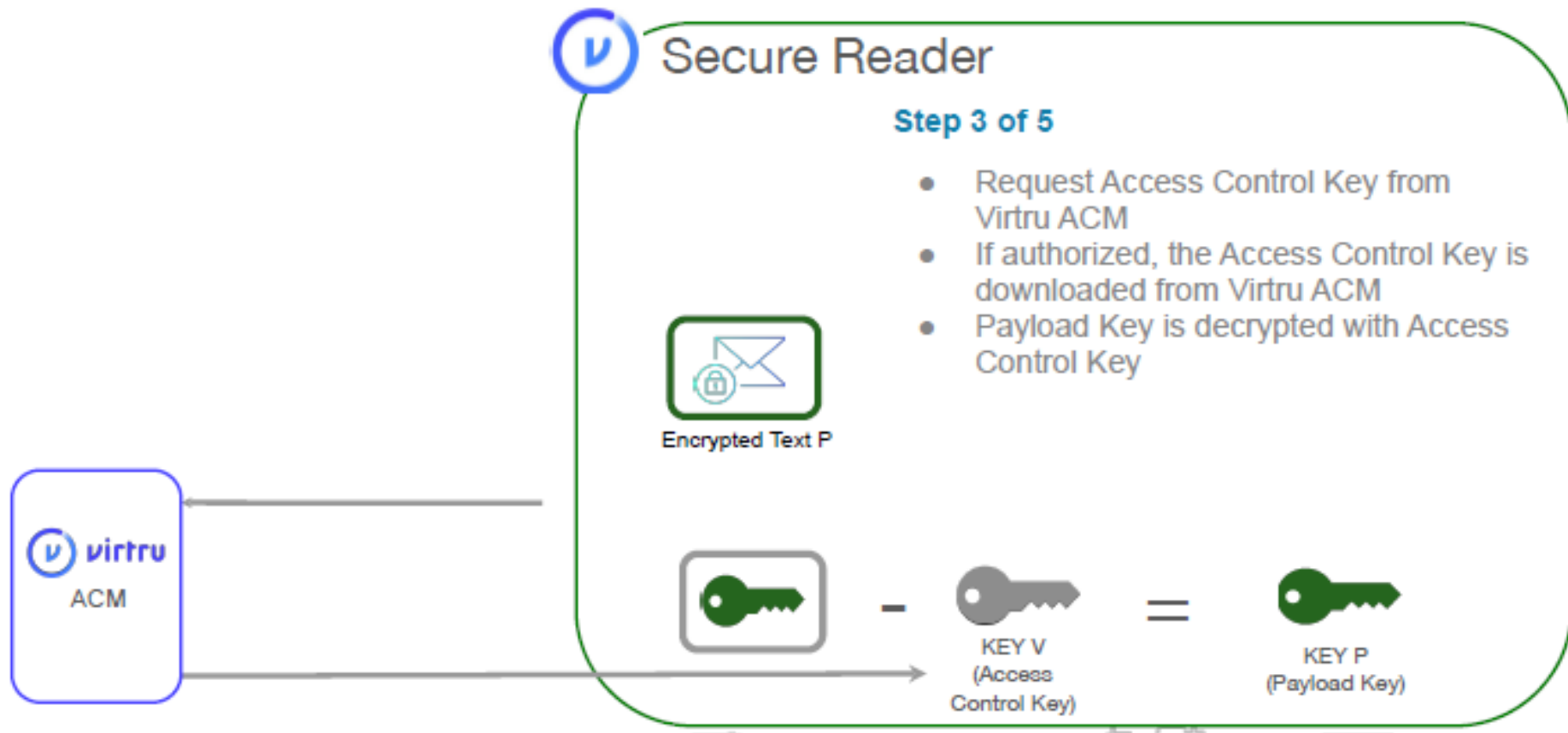
Virtru to non-Virtru



Virtru to non-Virtru



Virtru to non-Virtru



Virtru to non-Virtru



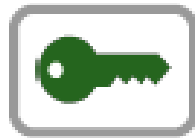
Secure Reader

Step 4 of 5

- Payload Key is decrypted with Access Control Key



Encrypted Text P



—



=



KEY V
(Access
Control Key)

KEY P
(Payload Key)

Virtru to non-Virtru



Secure Reader

Step 5 of 5

- Decrypt Encrypted Payload using Payload Key



Encrypted Text P

—



KEY P
(Payload Key)

=



Plain Text
Message



Sending Encrypted Mail w/ Virtru

Unencrypted

A screenshot of an email composition window titled "Test encrypted email". The window has a dark header bar with standard window controls. Below the header, a grey bar displays "Virtru protection is OFF". To the right of this bar is a red-outlined box containing a grey toggle switch with a "V" icon, which is currently in the "off" position. Below the grey bar, the "To" field contains "testuser@outlook.com" and the "Cc Bcc" labels are visible. The main body of the email contains the text "Test encrypted email".

Encrypted

A screenshot of an email composition window titled "Test encrypted email". The window has a dark header bar with standard window controls. Below the header, a blue bar displays "Virtru protection is ON". To the right of this bar is a red-outlined box containing a blue toggle switch with a padlock icon and a "V" icon, which is currently in the "on" position. Below the blue bar, the "To" field contains "testuser@outlook.com". The main body of the email contains the text "Test encrypted email" and "This is a test message." A "Customize Intro" link is visible at the bottom right of the body.



Sending Encrypted Mail w/ Virtru

Test encrypted email



Craft, John <john.craft@vita.virginia.gov>

Mon 3/5/2018, 3:29 PM

You; ☞



I use Virtru to send and receive encrypted email. Click the "unlock message" button below to decrypt and read my message. If you have any questions, please contact me.



Unlock Message

© Virtru encrypts emails to keep private information safe. Learn more at Virtru.com.

How should we verify
your identity?


LOGIN WITH Microsoft


SEND ME AN EMAIL



Sending Encrypted Mail w/ Virtru

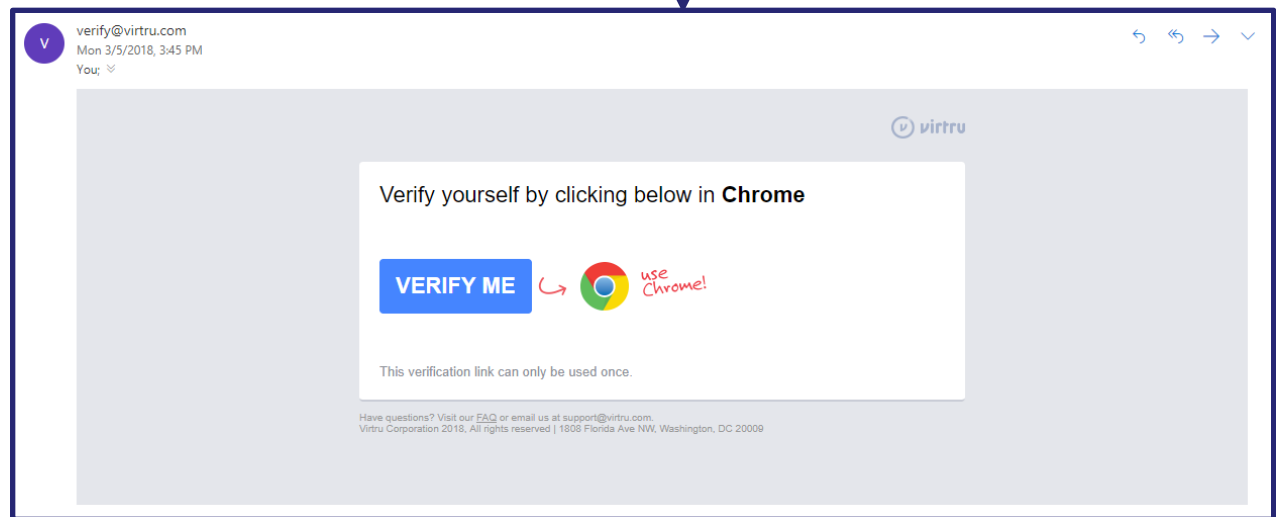
Select your email

 johncraft@outlook.com

 My Email is not here


☐ This is a Public Computer

☒ Remember me






Sending Encrypted Mail w/ Virtru

 **virtru** | SECURE READER

Test encrypted email
john.craft@vita.virginia.gov

To: johncraft@outlook.com
Monday, Mar 5, 2018 - 3:29pm

 Virtru Encrypted Message

This is a test message.

--
John Craft
Deputy Chief Information Security Officer
Commonwealth Security and Risk Management
Virginia Information Technologies Agency (VITA)
VITA - Powering the commonwealth's digital government
John.Craft@vita.virginia.gov
www.vita.virginia.gov
804-416-6032 voice
804-416-6359 fax


VITA Customer Care Center - Call (866) 637-8482 (toll free) to report an outage or request service. Or e-mail the VCCC at vccc@vita.virginia.gov. Please note: E-mail should not be used to report critical issues or outages impacting an agency. To report a critical issue, please call the VCCC directly.

Enter your reply here.

[SECURE REPLY](#)

Virtru respects your privacy. [Learn more about Virtru's privacy benefits.](#)

Secure your messages, control access, revoke at anytime. Get the free Virtru plug-in.

 **Get Virtru**



Virtru on Mobile

- Virtru is compatible with both iOS and Android
- This functionality is currently being assessed
- Some challenges with authentication
 - VITA is working with TN and Virtru to find a solution

Searching encrypted content

- “How can a search data encrypted by Virtru?”
 - Virtru tokenizes the content of the email body
 - Search tokens

`hmac_sha256(key, "hello")`



Hash

`sjzmverwjfb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824`



Search Tokens

`sjzm verwjfb0`



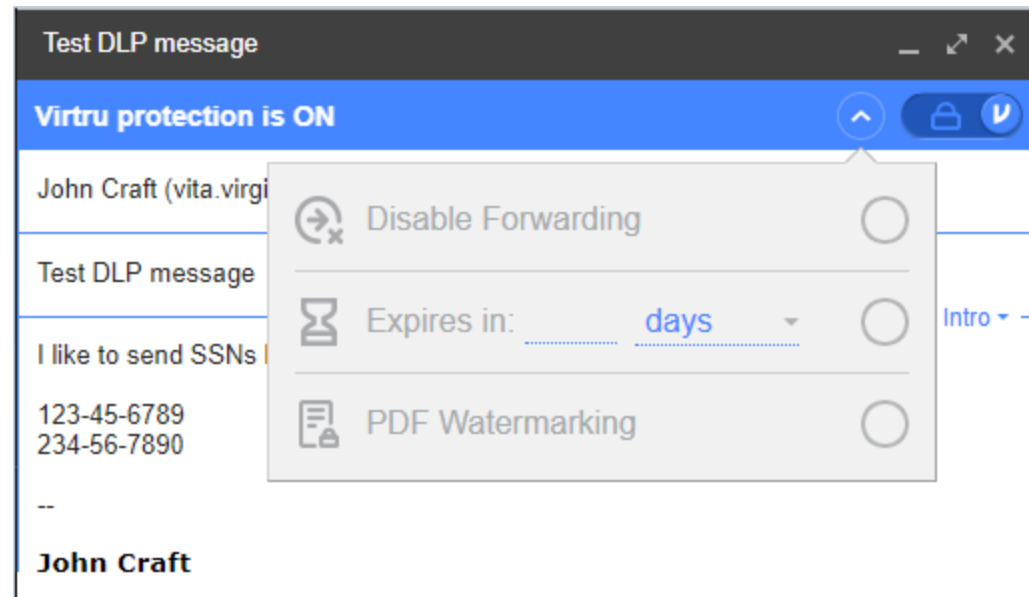
Searching encrypted content

- Every message encrypted by Virtru contains search tokens representing each word in the message body
 - Does not extend to attachments
- Search tokens are 4 characters long using [a-z 0-9], meaning there are 36^4 (46,656) possible tokens available
- Random search tokens are inserted into each message to prevent brute force attacks
 - Each message contains a minimum of 4665 tokens



Other Virtru Controls

- Disable forwarding
- Message Expiration
- PDF Watermarking
- DLP





DLP

- Both G Suite and Virtru have native DLP capabilities
- VITA is currently in process of replicating the existing enterprise DLP configuration into the new messaging platform
- Goal is to have enterprise DLP functional by the final message transition date (3/26/18)



Virtru DLP

Test DLP message

Virtru protection is OFF

John Craft (vita.virginia.gov)

Test DLP message

I like to send Social Security Numbers by email

Dummy SSNs:

123-45-6789
234-56-7891

--

John Craft
Deputy Chief Information Security Officer
Commonwealth Security and Risk Management
Virginia Information Technologies Agency (VITA)
VITA - Powering the commonwealth's digital government
John.Craft@vita.virginia.gov
www.vita.virginia.gov
804-416-6032 voice

Sensitive Items Found

Social Security Number

SEND SECURE **SEND**

[Cancel, I want to edit my email](#)

[Edit your rules on the Dashboard](#)

637-8482 (toll free) to report an outage or vccc@vita.virginia.gov. Please note: E-mail
es or outages impacting an agency. To report
ectly.

Automatic Protection*

Your Virtru extension detects sensitive content automatically. You decide what actions you want to take to protect your content.

*Virtru DLP is supported on G Suite, Gmail, Microsoft Outlook Web App for Office 365, and Microsoft Outlook 2010, 2013, and 2016.

Search subject lines, file names, or email addresses

| When I type these text patterns... (1) | Encrypt Email | Warn Me | Ignore |
|--|-----------------------|----------------------------------|----------------------------------|
| Credit Card Number | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Federal EIN | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| IP Address | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Possibly Sensitive | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Social Security Number | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |

| When I type these keywords... (1) | Encrypt Email | Warn Me | Ignore |
|-----------------------------------|-----------------------|-----------------------|----------------------------------|
| account number | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| confidential | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| FINRA | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| HIPAA | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Non Disclosure Agreement | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| off the record | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| password | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| PII | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| proprietary | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| subpoena | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |



Regulatory

- Virtru can be configured to meet or exceed requirements for the protection of FTI, CJI, and HIPAA data
 - Can be configured to comply with FIPS 140-2
 - AES-GCM 256-bit keys used to encrypt all data
 - Elliptic Curve Diffie-Hellman (ECDHE) is enforced for all communications, to include key exchanges



Questions

QUESTIONS?



Virginia Information Technologies Agency



Upcoming Events





Registration is Now Open

"2018 COVA Information Security Conference: "Expanding Security Knowledge"

April 12 & 13

Location: Altria Theater

<https://wm.irisregistration.com/Site/VITA2018>

Registration Fee - \$175

***Contact CommonwealthSecurity@vita.virginia.gov for more information**



Conference Keynote Speakers

Adam S. Lee,
Special Agent in Charge
Federal Bureau Investigations (FBI)
Richmond (Division) Field Office

Dr. Deanna D. Caputo
Principal Behavioral Psychologist
Human Behavior and Cybersecurity Capability
Steward
The MITRE Corporation



VITA Track

As part of the VITA Track, Bill Stewart, Service Owner will present on Generation Security.

This presentation covers future Security Provider/Security Services and Security in the future VITA model.



Future ISOAG

April 4, 2018 @ CESC 1:00-4:00

Speakers: Blake Carpenter, Grant Thornton LLP

Bill Freda, VITA

ISOAG meets the 1st Wednesday of each month in 2018



ADJOURN

THANK YOU FOR ATTENDING

