Building Nunavut Together
Nunavut Piqatigiingniq
Bâtir le Nunavut ensemble

ᐱᓕᕆᔨᒃᑯᑦ ᑐᖓᔪᓂᖅ
Technical Bulletin
Qaritauyaliqutinut Takuyauyaghat
Bulletin technique

Government of Nunavut Ransomware Report

July 14, 2020

Contents

Purpose of this Document (In-scope/Out of Scope)

The purpose of this report is to review the Ransomware incident of November 2, 2019, on the Government of Nunavut. This report is written entirely from the Community and Government Services (CGS) Information Management/Information Technology (IM/IT) perspective. The report will provide the background leading up to the event, details of the attack, and the remediation efforts undertaken to restore service.

This report does not detail the impact on any other Department or Organization within the Government of Nunavut (GN). For information related to departmental impacts, please refer to the individual departments.

Background

The delivery of IT for the government is considered a strategic corporate service. The IM/IT Division, within CGS which is led by the Corporate Chief Information Officer (CCIO) is the sole branch within the GN entirely dedicated to providing IT services for government across Nunavut. The delivery of IT services to GN departments and, in turn, residents of Nunavut is dependant on a hybrid network of effective and reliable satellite broadband, fibre optic cable networks as well as other support infrastructure.

Located in 25 communities across Nunavut and with southern Canada offices in Ottawa and Winnipeg, GN facilities share a sense of territorial isolation due to their remoteness and vast separation. Communication between all government offices is solely dependent upon satellite services with terrestrial connectivity established through specialized services from facilities located in Ottawa and Saskatoon. These realities have left the GN and all Nunavummiut with some of the most expensive and limited IT services in the country, specifically in telecommunications.

Despite these significant challenges, the IM/IT Division of CGS is making strides towards upgrading the GN's Information Technology infrastructures. These upgrades are significantly expanding corporate IT applications, network access, and internet connectivity services for departmental programs across all communities within Nunavut.

Government of Nunavut Ransomware Attack

On Saturday, November 2, 2019, a new and sophisticated category of ransomware affected the GN computer network territory-wide. The ransomware encrypted files on various servers, workstations, and external storage devices in the GN network. Once the threat was identified on November 2, 2019, IM/IT immediately took the network offline, identified affected services, initiated a contingency response plan and contacted cybersecurity experts and software providers to begin remediation efforts.

GN departments implemented contingency plans, ensuring essential services to Nunavummiut continued with minimal interruption.

A GN employee posted on Facebook about the ransomware attack on the Government of Nunavut and provided a picture of the ransom note as seen on their workstation display (See **Appendix A:** Ransomware Note on Computers and Published).

A decision was made by the leadership team not to pay the ransomware as, paying it would not have guaranteed full recovery of GN data, nor the future security of government systems. Once the decision was made, IM/IT initiated ransomware response teams to ensure network re-build, full systems data recovery from backups, and desktop remediation/rebuild for end users.

An emergency meeting of the Deputy Ministers was called to communicate the situation. All business units moved into their Business Continuity Plans (BCP) to ensure the continuation of services for all of Nunavummiut. IM/IT worked to provide support to all departments to ensure their BCP plans could continue. Under the direction of the Deputy Ministers Committee, essential services were identified that set priorities of services to be restored (Health, Family Services, Justice, Education, and Finance).

A communication strategy was implemented for Deputy Ministers to meet twice daily, share information, make critical decisions and provide updates on the recovery efforts.

Government of Nunavut Ransomware Response & Investigation

IM/IT initiated a full recovery from the adverse effects of the ransomware cyber-attack incident.

A plan was created to achieve full recovery of GN Network, systems, and rebuild workstations in all 25 Nunavut communities, including regional offices in Ottawa and Winnipeg.

Each stage of the plan consisted of specific tasks to be performed by IM/IT and reaching out to departmental resources for assistance where/when appropriate.

The strategy involved a parallel execution in a phased approach by splitting all available resources (IM/IT & departmental) into a backend restore group and three desktop teams. Each desktop team was assigned to a Nunavut region (Kitikmeot, Kivalliq or Qikiqtaaluk). A "war room" was established in Iqaluit as a command centre for the recovery of GN systems and to support the remote teams.

Iqaluit War room

IM/IT staff on charter to Grise Fiord to rebuild all community workstations. IM/IT staff visited all 25 Nunavut communities to rebuild GN user computers.

- The IM/IT management team, DM of CGS, and the Minister of CGS took on additional roles:
    - Minister of Community and Government Services took the role of informing cabinet and MLAs on the progress of recovery.
    - Deputy Minister of Community and Government Services took the lead role of the DMs oversight committee for the planning and execution of the recovery activities.
    - Corporate Chief Information Officer took on the business liaison role of point of single contact, working between internal IM/IT and the business departments, and with the DMs and Communications teams.
    - Director of Government Information and Planning took lead in the client terminals remediation (procurement, workstation rebuilds, and community deployment) for all communities.
    - Director Information & Communications Technology took the lead on the investigation, rebuild, server remediation and restoral of services for all communities.

IM/IT management met to evaluate the current state of the recovery. Although GN had specialists on staff, a decision was made to call in industry experts in malware attacks and aid in the investigation/recovery. RCMP also initiated an investigation on the attack on GN systems.

With answers from the investigation coming together rapidly, IM/IT backend restore team along with Teknicor as part of our managed service began the execution of the recovery of the GN networks and systems. In parallel the IM/IT frontend restore teams also began the planning and deployment of Windows 10 workstations in all 25 Nunavut communities and southern offices in Ottawa and Winnipeg. IMIT worked with various vendor such as Mandiant/FireEye (cybersecurity experts) and the Microsoft Detection and Response Team (DART) who are

leading experts in security and systems recovery validated the GN recovery plan as it progressed. The vendors also provided additional tools and assistance ensuring the appropriate security was applied (hardening) to the environment as well as the deployment of new cloud-based solutions for productivity and security. (See **Appendix B**: Microsoft Report)

The recovery execution was an all hands-on deck scenario. People were assigned different tasks that may not have been part of their normal job description to allow CGS IM/IT to move resources into jobs they would not otherwise do, but where help was required. The focus was on getting the primary data centre in Iqaluit back online so that all communities could connect into it for core business applications. Restoring GN applications in Iqaluit began with bringing government voicemail, systems, applications, and user data back online. The team in parallel began preparation to rebuild all other communities. The restoration activities included a full rebuild of the GN network in all communities, rebuild of all GN back-end systems, re-imaging of all GN computers to Windows 10 in all communities, and the deployment of new cloud based productivity tools.

The Government of Nunavut has very sophisticated backup systems. These systems are used daily to protect the Government of Nunavut data across the territory and in all government data centers. IM/IT created a segregated environment, disconnected from everything else, to restore the backups and ensure government data was safe. The teams filtered data backups through a variety of screening with FireEye to confirm they would not be restoring any infected or compromised files. The screening was successful. This process was very meticulous and time-consuming but critical to the success of the rebuild. Once confirmed the backups were clean, current (as of the end of day November 1, 2019) and accessible, the decision was made to recover/restore government data.

There were some exceptions to the loss of data:

- The data for Nunavut Arctic College – Multiview Accounting System had to be restored from the end of the day, October 31, 2019. This meant a one-day loss of data that would have to be re-entered manually.

- Data stored locally on “C” drives and not backed up by users to the network personal or shared drives.

- Data stored on USB and portable hard drives and not backed up by users to the network personal or shared drives.

GN Applications

As part of the rebuild process, the decision was made for any application to get back on the network, they must adhere to new strict security controls.

1. GN applications that met the new security control criteria were restored and brought online based on the priority of essential services first, then departmental need and application and data availability.

2. GN legacy applications that did not meet the new security controls, were placed into a secure zone on the network (behind firewalls) with strict user access limitations. IM/IT worked to bring these applications back online and notified client departments when these applications could not be put back onto the network as they were before, due to the security risk.

   The recommendation was made to work with the client departments and respective application vendors to find a viable solution for non-complaint departmental applications. These applications would either need to be enhanced to meet our new security requirements or be replaced.

3. Migrate productivity applications to the cloud.
   a. IM/IT determined the most efficient and secure way to bring back some enterprise applications was to move them to cloud-based solutions. These include:

      i. Office 365
         1. E-mail
         2. Microsoft Teams
         3. OneDrive
         4. SharePoint

The E-mail services were moved from an on-premise solution to Office 365 in the cloud, territory wide. With the implementation of Office 365, IM/IT enabled Microsoft Teams

application for instant messaging and video conferencing, SharePoint Online and OneDrive for file sharing and collaboration.

GN Workstations

In parallel to other backend activities, GN front-end teams in all regions began the rebuild of GN workstations. As most GN communities do not have Help Desk staff, charter flights and scheduled flights were arranged to bring all communities online. Teams were created in Qikiqtaaluk, Kivalliq and Kitikmeot regions to manage the workstation remediation. During the remediation, with the Windows 10 upgrade and new security enhancements, it was found that over 1400 workstations would not function or at very poor performance for users and were replaced as part of the rebuild.

Iqaluit, Rankin, & Cambridge Bay Workstation rebuild/replacement facilities – all workstations were collected and upgraded/replaced.

The logistical coordination for the procurement of workstations, shipping to communities, flights and hotels were all major challenges. Charter flights and scheduled flights were arranged to maximize the appropriateness of the teams to respond and bring all communities back online rapidly. The teams encountered many issues such as weather delays, aircraft mechanical issues, accommodation issues, and a medivac emergency commandeered one of the charter planes, just to name a few of the many challenges. By December 21, 2019, all Nunavut communities had core connectivity and access to GN systems.

Cost

In responding to the ransomware attack, GN has incurred costs in the form of overtime pay for staff, contract resources, replacement of over 1400 user workstations, charter/scheduled flights, new software licensing for new cloud services, and third-party security support services.

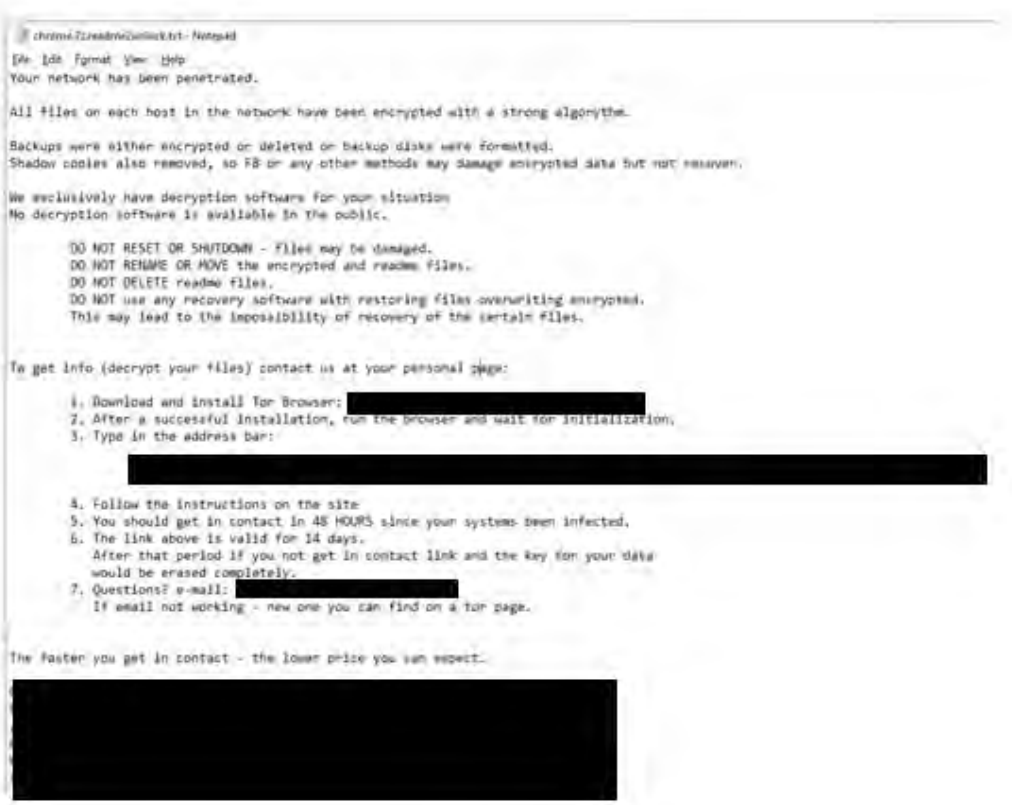
The cost associated for CGS IM/IT from the ransomware incident between November 2, 2019 to March 31, 2020 was $5,439,950 territory wide.

The people make the difference.

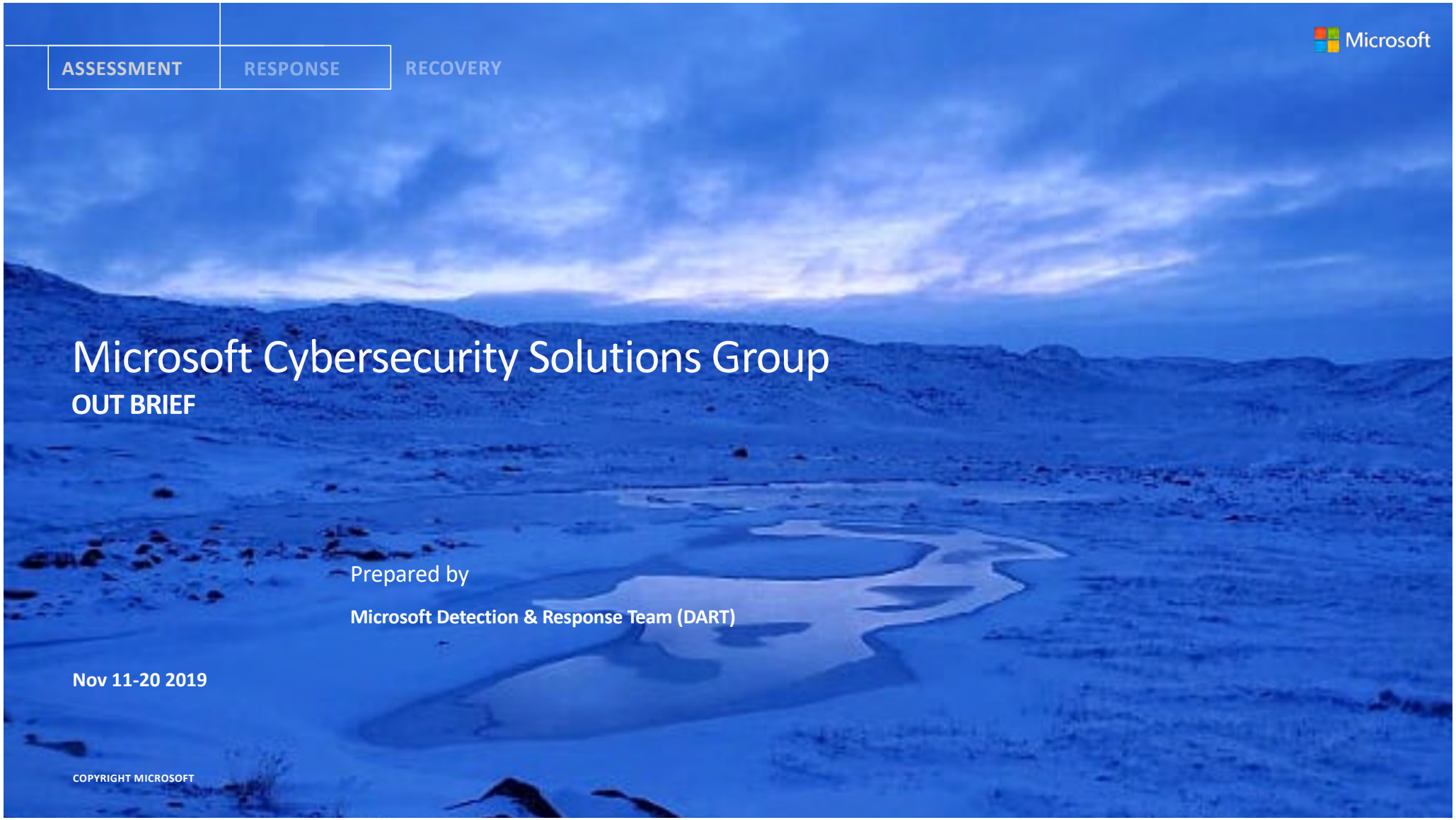
The Government of Nunavut Team

The GN was attacked by a sophisticated category of ransomware on November 2, 2019. Within 6 weeks, all Nunavut communities and southern offices had core connectivity with applications being brought online. The GN response to and recovery from ransomware was incredible! The people factor made the difference in the success of the GN recovery.

APPENDIX A: Ransomware Note on Computers and Published:



```
chrome.7z.readme.unlock.txt - Notepad
File  Edit  Format  View  Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: [redacted]
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:
                [redacted]
        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 14 days.
           After that period if you not get in contact link and the key for your data
           would be erased completely.
        7. Questions? e-mail: [redacted]
           If email not working - new one you can find on a tor page.

The faster you get in contact - the lower price you can expect.

[redacted]
```


ASSESSMENT
RESPONSE
RECOVERY
Microsoft
Microsoft Cybersecurity Solutions Group
OUT BRIEF
Prepared by
Microsoft Detection & Response Team (DART)
Nov 11-20 2019
COPYRIGHT MICROSOFT

Executive Summary

When Microsoft DART arrived on Nov 11th[th], a Doppelpaymer ransomware incident had recently occurred (Nov 1st). In addition to our typical incident response expertise, we were also tasked to assist with re-establishing business continuity and operations.

The current threat level for the environment based on the data collected is defined as **LOW**. This rating is based on the following:

- *Tier Zero Containment:* Steps were taken to isolate Tier 0 from attack, and to harden Domain Controllers
- *Local Administrators*: The Local Administrator Password Service (LAPS) tool was deployed across the enterprise, which significantly reduces the possibility for lateral movement by malware/Determined Human Adversaries (DHA)
- *Azure and O365*: O365 was deployed and email re-enabled, and Microsoft Defender ATP and Azure ATP were deployed, as well as Microsoft Cloud App Security (MCAS) and Azure Sentinel to provide visibility into activity across the entire enterprise.

'Patient Zero' for this incident was a workstation where a user clicked a link in a spearphishing email. The Dridex credential stealing malware was downloaded and two hidden system level accounts were used for lateral movement deployment of the Doppelpaymer ransomware.

During the course of this engagement, action was taken to identify Tier 0 assets (accounts and computers), and secure those assets using proven methods and 1)ensure Tier 0 accounts cannot login into lower-tier computers and 2)Lower tier accounts cannot login to Tier 0 computers.

Note: Ratings are intended as a "point in time" indicator of the customer's relative security posture but are not a guarantee for or against a compromise.

Incident: Timeline

Patient
Zero

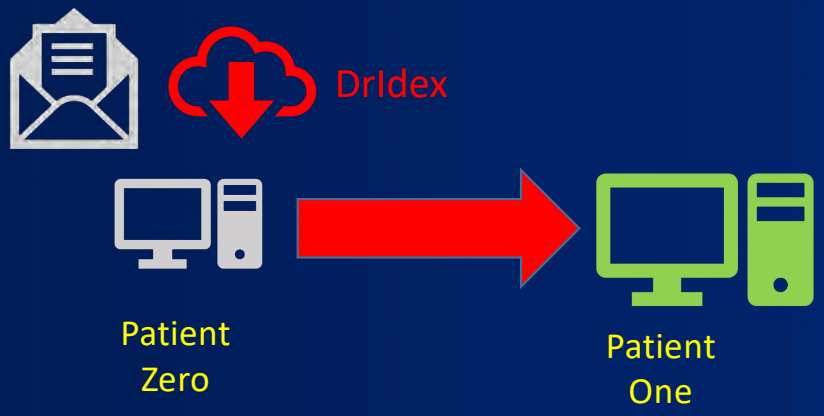
Incident: Timeline

Patient
Zero

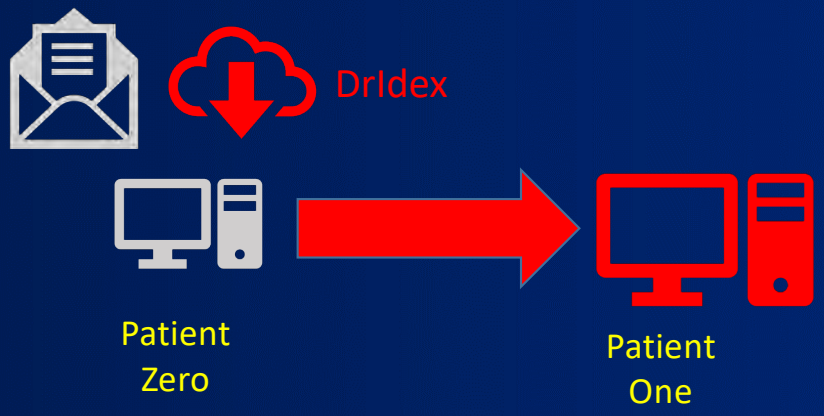
Incident: Timeline

Patient
Zero

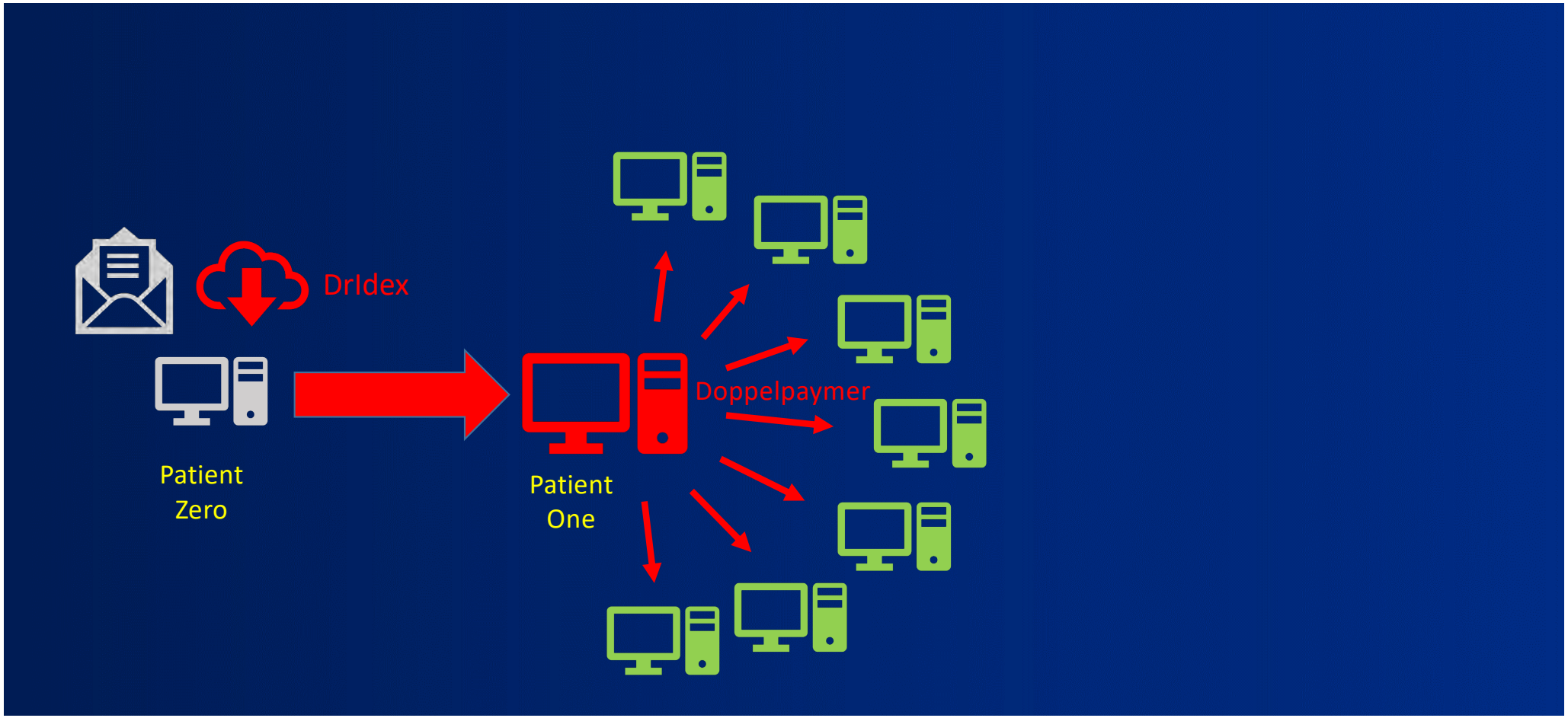
Incident: Timeline



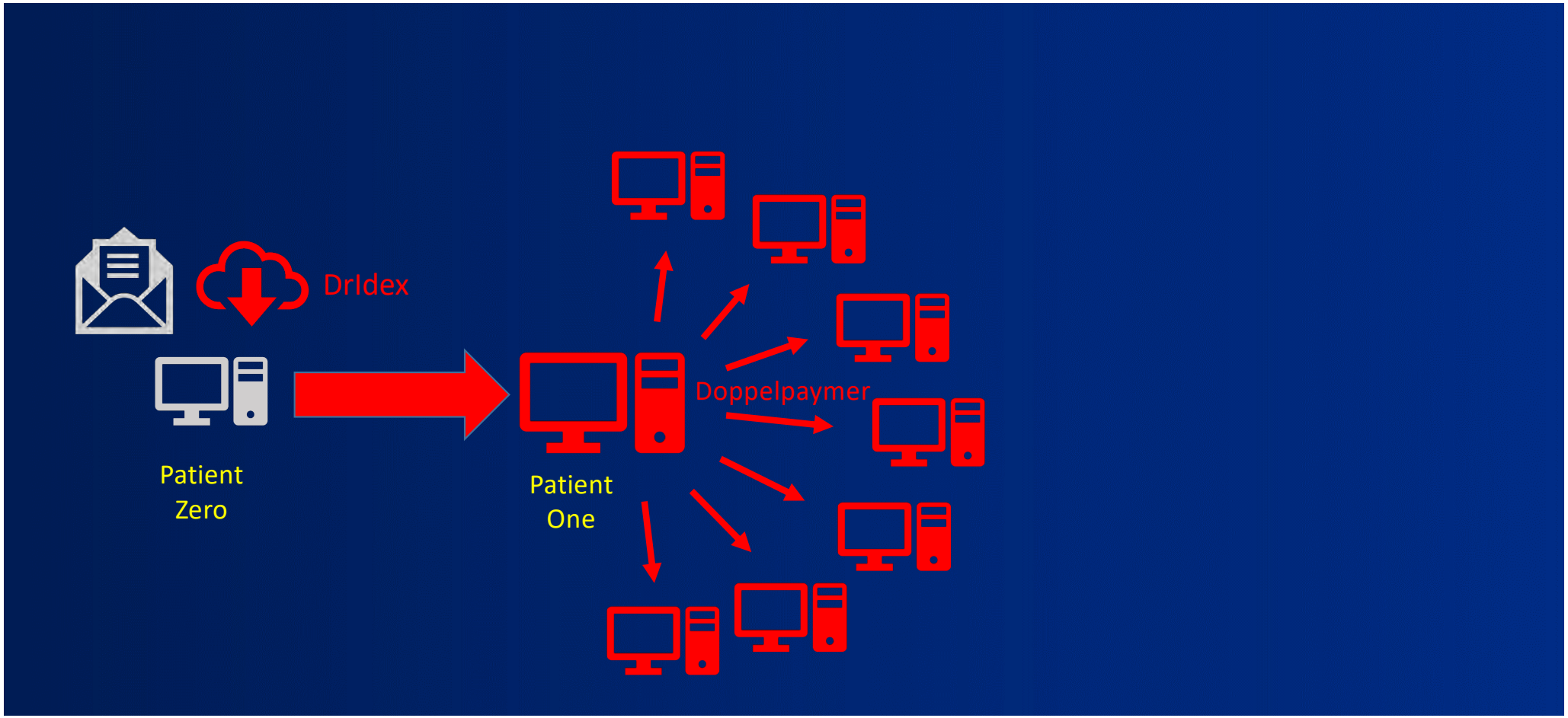
Incident: Timeline



Incident: Timeline

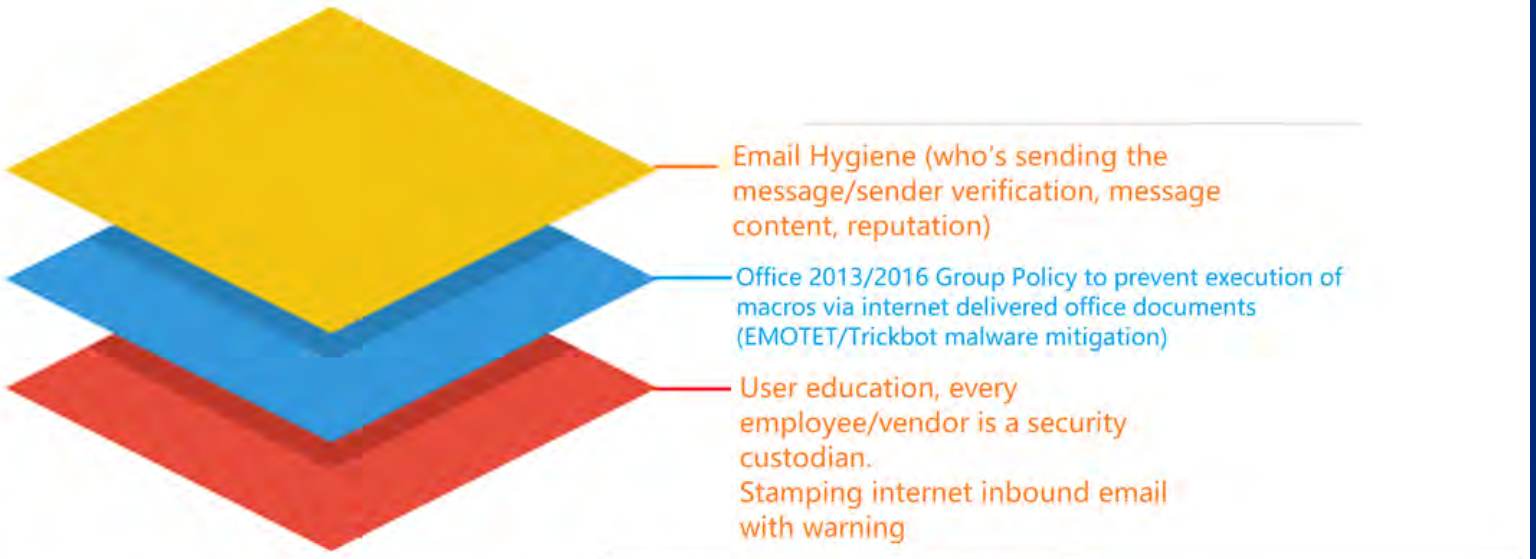


Incident: Timeline



Recommendations & Next Steps

Defense in Depth



Many layers/controls applied – collective strength

If one fails, other layers protects and mitigates

Recommendations

#Defense in depth

- Update all domains with email domain sender verification (3 domains pending SPF, DKIM is not currently applied to all domains
- Remove Email/Mailbox from all Global Admin Accounts
- Fix: Domain account admin was required for Dir sync when enterprise admin is only required (create a microsoft support case)
- deployed Exchange on-premises for scanners and internal email relay
- Transport Rule for internet inbound users warning users to be careful on clicking on links or attachments
- GPO to prevent execution of macros for internet based office documents (additional security training for users/business groups that require opening email based macro documents)

#Incident Response (Visuals have more impact over email)

- Online Microsoft Security Dashboards (Azure ATP, Defender ATP, Cloud App Security, Office 365, Azure Active Directory)
  - **create a single pane glass view** using (Security Graph API, PowerBI) showing heat indicators of suspicious behavior. LCD monitor in the IT area/raspberry Pi, etc.
  - **Posters at main entrances/elvators** advising on being a security custodian (do not use corporate credentials on 3rd party sites or clicking on links in suspicious emails
- Print copies of our Pass-the-Hash (PtH/Other Credential Theft Document, have it available to all support engineers. Provide a printed copy to new hires to explain assume breach and security tiers/network isolation.
  - Download from http://aka.ms/drew

Recommend follow-up with PFE/MCS for a cold eyes review: how you are using our security products to better optimize usage and visibility

Recommendations <most critical>

Patching

Implement a comprehensive patching strategy across all systems, for both Microsoft and 3rd party products. This is critical.

Active Directory Hardening

Continue implementation and refinement of Active Directory Administrative Tier model (0/1/2)

Restrict Service Accounts from interactive logins. Control using Conditional Access.

Standardize DCs and reduce attack surface.

Enable MFA

Implement and Enforce multi-factor authentication (MFA) for DA/EA and cloud accounts, and 100% of VPN users.

Microsoft Defender ATP

Enroll 100% of computers in Microsoft Defender ATP.

Actively monitor alerts and quickly take action on issues in the console.

Leverage Microsoft Threat Experts for monitoring.

Modernize Windows

Continue to deploy Windows 10 and Windows Server 2019 to enterprise before the end of 2019.
(Windows 7 and Windows Server 2008 reach EOL 14 Jan 2020).

Maximize Windows 10 Functionality

Enable Credential/Device/Exploit Guard, Windows Hello for Business, SmartScreen, Application Control, Controlled Folder Access, Attack Surface Reduction, Bitlocker, Secure Boot, etc..

Recommendations <also critical>

Manage Legacy protocols

- Disable SMBv1
- Disable NTLM
- Discontinue use of TLS 1.0 and 1.1 (EOL 1st half 2020)
- Update all services & apps which use SMTP, Telnet, FTP, Imap, etc. to modern non-clear-text alternatives. This is *required* to disable Legacy Authentication in O365, which is required for Conditional Access

PS and CMD logging

- Central logging of command line tools provide an archive of activity.
- Update Powershell to latest version for additional functionality

Privileged Access Workstation (PAW)

- Plan deployment of Privileged Admin Workstation (PAW) for EA/DA T0, T1, and Azure admins.
- **Monitor T0 accounts and audit usage regularly.**

Credential Hygiene

- **Continue Credential Hygiene Best Practices**
- **www.aka.ms/tier0 for reference materials**

Recommendations <also important>

Inventory Applications

Enable Applocker in Audit Mode to inventory applications.

Analyze and blacklist unauthorized applications.

Ideally, whitelist approved applications.

Group Policy Review

Perform Group Policy Risk Assessment Program to analyze and optimize AD Group Policy.

Enforce Windows Firewall

Windows Firewall protects computers from network attacks

Monitor changes to firewall configuration on endpoints

Establish Comprehensive Incident Response Plan

Continue to formalize plans for future Security Incidents, including host isolation, out-of-band communications, quick implementation of change, etc.

Microsoft Azure ATP

Monitor Azure ATP for unusual login activity and advanced attacks (Golden Ticket, Skeleton Key, Pass-The-Hash, etc.)

Plan to secure Tier 1

Same steps we put in place for Tier 0, look into how to secure your most critical, high value asset systems in Tier 1.

Recommendations <also important>

O365 Recommendations

- Require MFA for O365 users
- Move from on-prem Exchange to O365
- Disable Legacy Authentication
- Embrace Conditional Access
- DART O365 Review is available

Maximize MSFT services

Microsoft Premier Field Engineers and Microsoft Consulting Services are available to help with all of these recommendations

DART 'Cybersecurity Operations Service' (proactive version of Incident Response Service) is available

Continuous Security Monitoring

Ensure that sensors are monitored 24x7 and that actions are taken on alerts in a timely manner.