The MSB 2018 Virus Situation

As of July 30

By Eric Wyatt, IT Director, Matanuska-Susitna Borough

The Attack

Information about the attack has been widely shared with other agencies to help them prepare and hopefully avoid a similar attack. These efforts have been greatly appreciated by these agencies.

This was a multi-pronged, multi-vectored attack. Not a single virus but more generally, ***Malware***. Aspects include: Trojan Horse (Emotet), Worm, Crypto Locker (Ransomware (BitPaymer)), Time Bomb, Dead Man's Switch, External hacker logged in to our network, maybe more . This is an ***Advanced Persistent Threat.***

This is also a ***'Zero-day'*** attack. Meaning, the anti-virus software does not yet have the virus definitions in their software to catch and remove this threat.

Most probable method of initial delivery is email with a hyperlink to an infected website and prompt to install an add-on or with an attachment with a macro. Users with local admin permissions are most at risk.

The FBI reports: Once the Trojan component is inside, it opens the door for the hacker and brings in the other viruses. Then it uses the user's Outlook contact list to send itself to other government looking addresses. The *From* address is most likely from someone you know and trust.

Once inside the virus/hackers work to gain Active Directory administrator access. They then '*own'* the Domain controller, drop all internal security settings, logging, and auditing, which is then spread to all servers and workstations through normal Active Directory mechanisms. They then can easily crack all passwords and spread to all machines.

These viruses appear to be written in Microsoft Visual Studio (common developer's tool) and attack only Windows based machines.

This attacks appears to have been lying dormant and/or undiscovered within our network since as early as May 3rd.

During this time, data from any of our systems may have been compromised and sent outside of our network. We do not have evidence of this, but **we must work from the assumption that this was done.**

Everything we have seen matches the patterns the FBI has seen at multiple sites throughout the country. It also matches the situation in Valdez.

The FBI reports that the Trojan and Worm will lay dormant for 4 to 6 weeks and then the Crypto Locker component is frequently launched on a Friday. This happened in Valdez and there are reports that on Friday multiple other locations in Alaska and around the US were hit.

We started to pick up Trojan component of the attack on July 17th after an update of our anti-virus software (McAfee). This was only seen on Windows 7 machines. McAfee was then doing its job of detecting and deleting the Trojan, but continued to miss all other components. By the time the number of workstations affected rose to alarming levels, we had discovered the same issues on multiple servers. We developed a script to remove the discovered components that McAfee was leaving behind from all machines and planned to launch this on Monday evening, July 23rd. We also expired all user passwords to force password changes and changed passwords for all admin and service accounts.

This action, of attacking back, seemed to trigger the virus to launch the Crypto Locker component. This trigger may have been automated, a *Dead Man's Switch*, or there may have been a person manually monitoring activity and executed their Command and Control (C2) to launch the attack.

The Crypto Locker then began encrypting files on workstation and servers. Nearly all of the 500 workstations (both Windows 7 and Windows 10) and 120 of the 150 servers have been infected.

This encryption is portrayed as a *Ransomware* attack, however, its real purpose may be to cover the tracks of the other components. Files, logs, scheduled tasks, executables, and other evidence, if found, can point investigators to the people responsible for writing the viruses. Even the language the virus is written in can point to the country of origin. This scenario is supported by the fact that even when the ransom is paid, the decryption codes are never given. This would indicate that the attack's purpose is not based primarily on money from a particular victim, but to disrupt operations and potentially steal information that may lead to greater financial reward and more disruption from down stream victims.

At this point we notified the FBI and began to communicate with other affected and interested agencies. We also formed teams to deal with the containment, analysis, and recovery.

To date, many agencies, companies, and organizations have participated in or offered help for this effort at the Mat-Su Borough: MSBSD, FBI, GCSIT, MOA, Resource Data, Inc, Wostmann and Associates, 5 Star Team, ACS Communications, Structured, Threat Informants, City of Valdez, State of Alaska, Alaska USA, Denali FCU, Mat Valley Credit Union, State Farm Insurance, ATS, Cisco, FBNSB, Dell, Commvault, Deeptree.

The external connection to the Internet was completely disconnected. Servers were first disconnected from one another and then completely shutdown. All work stations have been disconnected, shutdown and collected.

Current Condition

The External web site was not affected and remains active.

Almost all Windows based production servers have been encrypted, this includes our domain, email (Exchange), Govern, Logos, TRIM, SharePoint (intranet and eCommerce), GIS, SQL databases, S:\ drive files shares (L:\, M:\, P:\ ) and even our backup and Disaster Recovery (DR) servers.

The backup and DR servers had been engineered in a way that no known threats would affect. This new threat has always been considered a ***Theoretical Exploit***. To date, neither our local

network engineering consultant nor the international vendors: Cisco, Dell, Commvault, that they represent have seen this exploit developed and used. Further, our backup and DR model uses a multi-tiered approach to data protection, which appears to have saved some portion of our data, even under this sophisticated attack.

The phone system (Mitel) was encrypted, we lost some functionality but most direct lines continued to work as long as the phone was powered on.

The door lock card swipe system (Lenel) has also been encrypted but will continue to function in the last known good condition.

Though it initially appeared that our data was a complete loss, we have recently recovered data from the shared drives, Logos, Govern, TRIM, GIS and more.

eMail (Exchange) does appear to be completely unrecoverable.

Email as of last Tuesday has been spooling on our external email filter device. We have stood up an external web based mail spooler with all of our matsugov.us mail addresses. We can send and receive emails with this. It is a bit of a clunky interface. See attached instructions for use. This mail will flow to the new Exchange server when ready.

The Mitel phone system server has been rebuilt, we have recovered the data (configuration) and should have working phones on desktops Monday in DSJ and some remote sites. We have teams to continue to work phones at the remote sites.

We have about 110 workstations that have been cleaned and reimaged and are ready for placement. They are being processed according to the priority list. A copy of the infected data on the hard drive is being kept for potential data recovery and FBI investigation. These machines will be placed on a 'Green' network, meaning it is clean with no infected computers. They will be part of a workgroup, not a domain. This will come later this week or next. They have MS Office application and internet access. Clean data requests will be filled on these machines as soon as possible. They are being placed in DSJ and remote sites along with the phones as described above.

My Property on the external website has been restored with static data.

Logos has been restored on an external web service with 1 year old data. Current Logos data looks to be recoverable on the DR server.

Govern data has been restored to an external web service that is 1 month old. Current Govern data looks to be recoverable on the DR server.

The MSB domain was rebuilt Sunday.

Portions of the network have been redesigned and augmented to deal with this new and emerging threat by adding technique and software that is newly available.

Virus files have been set to McAfee so they can add functionality to our AV software to prevent further attack. We are awaiting the reply.

Computers and images have been given to the FBI for analysis. Also, all encrypted and other server and workstation files and images are being saved for the FBI.

Critical GIS data has been saved offline and can be restored to rebuilt systems. Maps, MXDs, parcel fabric, etc.

Going Forward

Additional desktop workstations will be reimaged and placed on desks at a rate of 38 per day or more (10 more days)

Workstations will be added to the MSB domain starting this week.

The Exchange email server will be built early this week. Workstations added to the domain can then use Outlook for e-mail and calendaring. Old email will probably not be available but functionality will be restored.

Work on damaged DR servers continues, functionality is coming back, and there is optimism for the recovery of additional data.

New, more secure servers will be created and enterprise systems will be rebuilt and hopefully will have data restored. Govern, Logos, GIS, SharePoint, TRIM, MPulse, iSupport, etc. This can easily take 2 or 3 more weeks.

Policies and procedures will be implemented in the Borough to reduce the risk of further infection and reduce the spread of infection should any other systems be hit.

User education training will be conducted on a periodic basis to help users avoid threats.

Encrypted data will be stored for months or years in hopes that the FBI will recover the decryption keys.

We will continue to participate in information sharing meetings to help educate the community against further attack.

-end-