



NEW HAMPSHIRE MUNICIPAL ASSOCIATION

NEW HAMPSHIRE MUNICIPAL ASSOCIATION
Celebrating Seventy-Five Years
of Service to Your Hometown



The Growing Threat of Ransomware

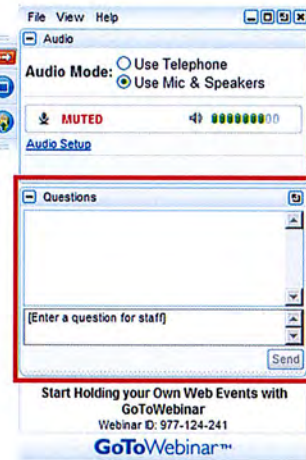
Presented by:

Erin Makarow, Marketing Coordinator, RMON Networks
David Cohen, Senior Services Manager RMON Networks
Chris Chaves, Senior Sales Engineer, Sophos

October 12, 2016

How to Participate Today

- Open and close your Panel
- Submit text questions
- Couple of questions for today
- Q&A addressed at the end of today's and/or during session at presenter's discretion



We have your City.
pay UP, OR eLSe!

Erin Makarow,
Marketing Coordinator,
RMON Networks



RMON
NETWORKS



My name is Erin Makarow, and I am the Marketing Coordinator for RMON Networks. If you haven't heard of RMON Networks, we have been providing I.T. Services to Municipalities since 2002, and we have been fortunate to be working with the NH Municipality Association for several years now. Last year I had approached Tim Fortier at the NHMA just shortly after the media started reporting that the Town of Tewksbury, MA P.D. had contracted ransomware. The Tewksbury PD was not prepared to combat this virus at all, and ended up paying the ransomware. It was a very public event. I hate hearing stories like that one, I feel like there is so many ways we can help. So I thought.. You know.. I am going to call Tim at the NHMA, and ask if there was something I could do to help make Towns aware of this issue... so to make a long story short, RMON Networks has been writing the Tech Insights column for the NHMA's Town and City Magazine for a little over a year now. Back then it started with a ransomware article, and now here we are... talking about this growing threat in more depth.

What Topics Would You Like to See Covered in the Tech Insights Column in *New Hampshire Town & City Magazine*?

Ransom Note

1. Moving email to the cloud
2. Moving servers and infrastructure to the cloud
3. Utilizing "Hardware as a Service" to update outdated PCs, servers.
4. How to deal with growing data storage
5. VoIP Phone Solutions
6. The value of a Network Audit
7. What you should look for, and expect from a Managed IT Service provider.




Before we begin. I was to take a quick poll from our audience. What other technology topic would you like to see featured in Town and City Magazine?

We haVE yOUr City.

pay UP, OR eLSe!

Ransom Note

 **OCTOBER IS**
National Cyber Security
Awareness Month

OUR SHARED RESPONSIBILITY



Before we jump right in here, I just wanted to stop and point out that October is cyber security awareness month. So we really picked a perfect month to all gather here and talk about ransomware.

History of Ransomware

Ransom Note

HISTORY

The first known ransomware was the 1989 "AIDS" trojan (also known as "PC Cyborg") written by Joseph Popp.

```
ATTENTION
I have been selected to inform you that throughout your process of
collecting and marketing files you have accidentally infected
several more users than I intended. Please, if you
can, let me know if you have infected your system. You can
also have me let about their addresses. You will not be
rewarded, thank it please for
```

AIDS



1st piece of ransomware was written in 1985, it was a Trojan called the Aids Trojan or PC Cyborg, it encrypted data on a hard disk, and physically asked people to send money through the US mail. Does anyone else see the problem with this???? We know where they are, we have their address! Since it was easily traceable because we had a physical address, the concept of ransomware didn't evolve. BUT when bitcoin came about, the playing field really changed. This is when ransomware revolutionized cyber crime, and has recently been reported as the most profitable scam in history. AND nobody is immune, agencies, and entities of all sizes have been reported victims with incidents escalating at an alarming rate. The FTC reports incidents quadrupling this year alone to on average 4,000 a DAY. Ransomware will continue

Why Would Hackers Target State and Local Government?

Larger government agencies, like larger private-sector businesses, have the

Ransom Note

A hand in a blue suit sleeve holds a white rectangular sign with the word "transparency" written on it in a black, sans-serif font. The background is a dark blue gradient.

transparency



<https://gcn.com/articles/2016/08/01/ransomware.aspx>

You may ask yourself why would a local government office be a target? Ironically, as I was creating this presentation the owner came over and dropped the latest edition of GCN Magazine on my desk. It's a technology for government focused magazine. Ransomware targeting governments was this month's main focus. Here you can see a power message they are delivering. Here you are being described as "easy pickings". Why are you easy pickings? According to GCN Magazine, most agencies do not have the technology currently in place, and are not prioritizing the technology in their budget. We want you to know that there are programs and products out there, that you can implement within a smaller, planned budget. AND Hopefully you will have many takeaways from today's presentation to get you started.

We have your City.
pay UP, OR eLSe!

David Cohen,
Senior Services
Manager,
RMON Networks



RMON
NETWORKS



At this point I am going to hand this presentation over to David Cohen, David is our extremely talented service manager here at RMON Networks. David Cohen has over 2 decades of industry experiences and too many certifications to list with Microsoft, Dell, Citrix, and more. He is here today to talk about technical steps and measures you can take to prevent ransomware.

Webinar Agenda

Ransom Note

- A. How do ransomware extortionists gain access to business computers?
- B. Are there business and technical measures you can take to prevent ransomware?
- C. What role can employee education play in preventing ransomware infections?
- D. Are there tools that municipalities can employ that will warn if their data is about to be encrypted?
- E. If you fall prey to ransomware, should you pay the ransom?
- F. Q&A with our security experts.



Here are the items we are going to cover in our presentation. We have a great mix of attendees today, so we are going to cover a few basics to start off with, and then get in to some technical items later in the presentation.

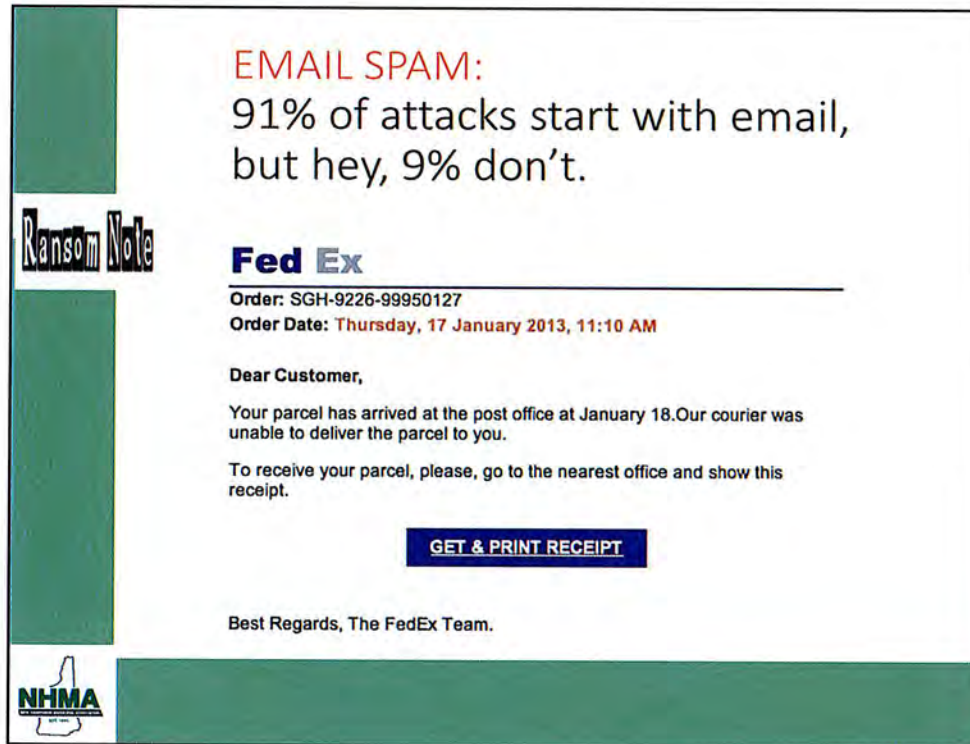
We have your City.

pay UP, OR eLSe!

Ransom Note

**How do
ransomware
extortionists gain
access to business
computers?**





The unwanted commercial email – also known as "spam" – can be annoying. But worse, it can include bogus offers, or malicious links – and is a widely used to spread ransomware. Pictured here you see one of the most common scam emails .. This one is a "Brand Scam" and is especially popular in the holiday season. I think we take for granted that everyone is aware of these types of emails, but we really need to create more awareness in the workplace, and that is something we are going to get in to in the upcoming slides.

PHISHING:
even worse spear phishing attacks

Ransom Note

Update your account L...
Outlook Item

Thu 10/12/2015 2:42 PM
conform your account <ssani@sani.com>
Update your account to avoid limits

to: ASIN@zpsnet

Update your details for PayPal

We need more information from you

Just like a bank, we need to confirm the information you've given us. Please provide the requested information as soon as possible to ensure you can continue to use your PayPal account.

You have 48 hours to provide this information. If we don't hear from you by then, we'll need to restrict your account. If your account is restricted, you won't be able to send, transfer or receive funds.

[Update Now](#)

Yours sincerely,
PayPal

More information

Copyright © 1999-2015 PayPal, Inc. All rights reserved.
PayPal Australia Pty Limited ABS 93 111 195 359 (AFSL 304962). Any general financial product advice provided in this site has not taken into account your objectives, financial situation or needs.

[NHMA Hook, Line and Sinker Article link here](#)

NHMA

Spear phishing preys on the familiar. It is banking on the fact that the user is going to believe what they are seeing is legitimate. It can be from a familiar website, like that PayPal request you see above. It's also very popular to receive an email from a co-worker, or boss requesting access to something, or money to be transferred. All this information is really easy to gather on social media. In fact, I can go to LinkedIn right now, look up a company, and find out who the accounting manager and president are within about 1 minute. The information is already out there, and readily available to the hackers. You see, hacking is just as much about people, as it is about code. Phishing attacks According to the FTC, 93 % of all spear phishing emails contain a ransomware virus.

Greenland, NH received an email posing as AT&T and had a voicemail for the employee. Another town received an email that appeared as though it was from virtual town hall websites. Opened the attachment, and the PC was infected!

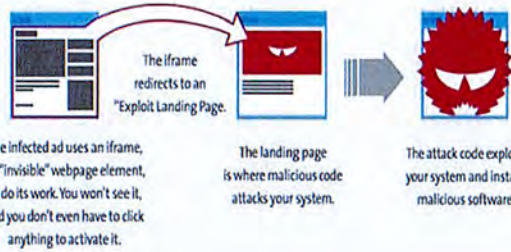
These criminals just keep getting smarter – How did they know to pose as a company frequently used by towns?

MALVERTISING

Ransom Note

HOW MALVERTISING WORKS

You visit a website with an infected banner or popup ad. No site is safe, no matter how legitimate it appears to be. Even mainstream sites such as NYTimes.com, Gizmodo, and Dailymotion have unknowingly carried infected ads.



The cyber criminal is banking on the fact that you feel safe on a Trusted Companies website. BUT.. Any website can be infected by Malware.

Roughly 90,000 people a day are redirected from malvertising to a single proxy server. 10% of those, or 9,000 are vulnerable to an exploit (system vulnerability), of that 40% were compromised.

\$34 million dollar per year

Exploiting system weaknesses

Ransom Note



*Source: Infoworld



Ransomware attackers are no longer limited to drive-by downloads, preying end-users to inadvertently click on the wrong link.

SamSam ransomware is a new and improved string of ransomware. Designed to get a foothold inside the organization by exploiting known server vulnerabilities. Server vulnerabilities, exist in outdated systems, unmanaged systems.

The fact that SamSam targets servers makes it easier for the ransomware to cripple an entire department or organization, as the data on the servers are mission-critical to running a business. It's so much more than the users PC.

While SamSam ransomware is the most immediate threat targeting web based servers, it isn't the only attack to worry about. Nothing is preventing attackers from using a compromised server to then launch denial-of-service

attacks or consume resources to mine bitcoins, for example.

We cannot stress enough the importance of patching software regularly and on time. Patching is critical but frequently neglected -- by organizations and by the software vendors themselves. Some of the SamSam attacks exploited weaknesses that should have been patched 7 to 9 years ago! According to a scan by cisco there are approximately 3.5 million vulnerable machines out there.

***Not keeping up with security patching can have a devastating impact on an organization.

Ransom Note

How to reduce your business risk and suggested technical implementations



Normal Glass



Bullet proof glass consisting of normal glass (blue) and polycarbonate (red) layers



RMON's recommended Seven Layers of IT Security

Ransom Note

- Email Security
- Next-Gen Firewall Security
- Domain Security
- Windows Security
- Endpoint Security
- User Awareness
- IT Governance



What is "Network Hygiene". Good network hygiene is really about keeping your network up to date and clean. Knowing your inventory, users, devices that are connecting, where your data can end up. It's really understanding what you have going on in your computer network.

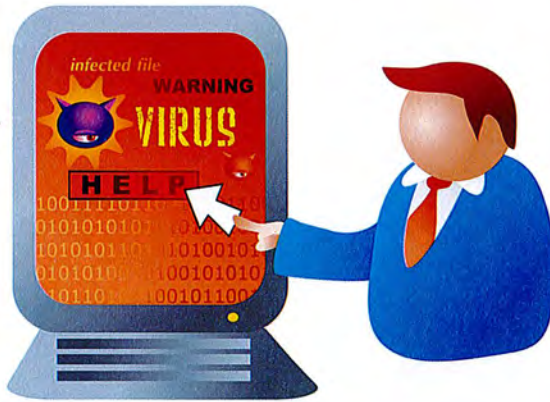
According to the Online Trust Alliance, 90% of all ransomware attacks could have been prevented with good network hygiene.

With that being said, you really need to focus on hygiene and prevention, because once you are hit, it's pretty much impossible to get your data back. With that being said... You need to have a backup.

Email Security

Ransom Note

- Spam filter
- Email link scanning
- Extension blocking



Next-Gen Firewall Security

Ransom Note

- IPS/IDS
- Web Filtering
- Download and Email Scanning
- Blacklisting
- Access Controls



Domain Security

Ransom Note

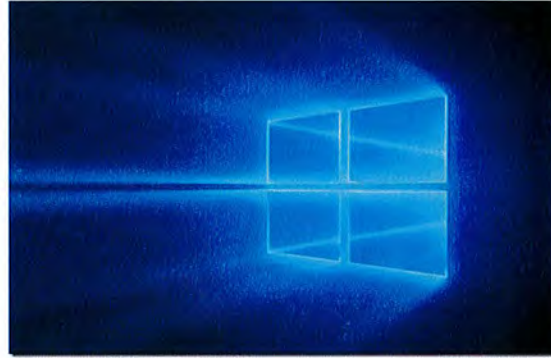
- Complex Password Policies
- Software Restriction Policies
- Share and File Security
- Disable Default Accounts
- Domain Auditing



Windows Security

Ransom Note

- Windows Patching
- Port Hardening
- Disable Windows Scripting Host/VBS scripts
- Limit Domain/Local Admins
- Show hidden file extensions
- Modern Browsers



Endpoint Security

Ransom Note

- Antivirus and Anti Malware
- Sandboxing and Host Intrusion Prevention Systems
- Browser Plug In Patching
- Disable Autorun on drives
- Disable Autoplay in browsers
- Enable Addblocking
- MDM



Governance

Ransom Note

- Monitoring
- WISP
- BC/DR Planning

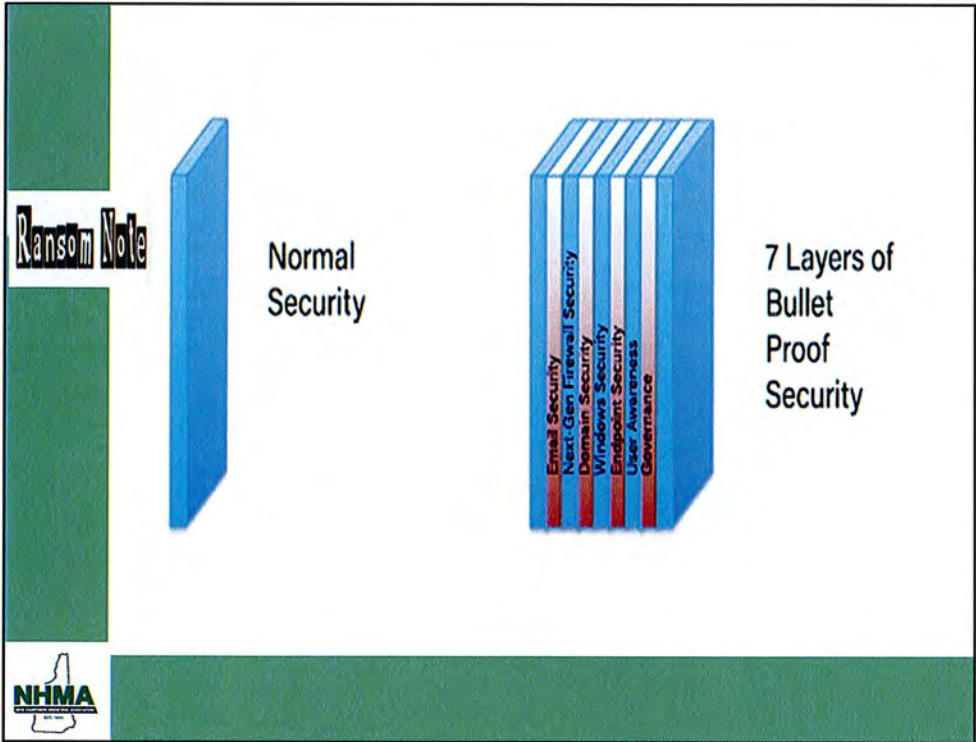


User Awareness

Ransom Note

- Malvertising and Phishing Education
- Device security and usage training





Ransom Note

What role can employee education play in preventing ransomware infections?



Hacking is just as much about people, as it is about code.

Ransom Note

95% of all successful cyber attacks is caused by human error

NHMA

As I stated earlier "hacking is just as much about people, as it is about code". We cannot stress enough promoting employee education & simple awareness programs. We all assume people know when something is a scam... but if that were true hackers would not be as successful as they are.

Awareness & Training Kit For Employees

Ransom Note

- Instructions on what is included and how to use
- PowerPoint Presentation
- Poster to hang around the office
- Buy in email to send to managers so you are all on the same page
- Email series with simple security tips to send out once a month.
- More



We have been providing a great user training kit for FREE on our website for quite a few years now. It is completely editable, so you can brand it yourself. It has everything you need to start an awareness program in your office.

Launch Guide Sample

Ransom Note

- Pick the pieces you want
- Edit them with your logos, additional info if you want, etc
- Launch and repeat



Step 1: Find advocates

The principals in your organization need to know you're doing this and they'll be glad you are. You know that data breaches can cause them all sorts of problems and they're the ones responsible for regulatory compliance.

It's great to get all management on your side so people take your plan seriously.

It's a good ally for this too.

Step 2: Choose your tools

Use as many or as few of the tools in our IT Security Dos and DON'Ts kit as you want. We've tried to make it as complete as possible.

Step 3: Make it your own

If you want to customize the various pieces in the kit, feel free. This is your program, after all.

IT Security Dos and DON'Ts Launch Guide

Step 4: Make a game plan

It's a good idea to create a plan so you can teach your people one up at a time. If you do it this way, they're more likely to remember what you tell them.

Whether you do it weekly or monthly doesn't matter. Doing it regularly does.

Send out the security tip emails. There's copy in the kit to just cut and paste and send off immediately.

Back it up with the posters that are included placed where people meet.

Step 5: Launch

Send a launch email. There's a sample one in the kit too. Attach the IT Security Employee Handbook.

Step 6: Reinforce and repeat

Repeat, repeat, repeat. You can't tell people often enough to be safe. Make sure they know that this is just as important to them as home as it is at work and you've got a better chance of them taking notice.

As threats and security issues evolve, we'll be updating the tool kit and creating more tools for you to keep your business and your people safe.

You're trusted partner

RMON
NETWORKS



We have some samples here of what is in our training kit. You can use this as a starting point. Change, or add what ever you'd like.

Sample of an email within the training kit

Ransom Note

Stay alert and report Suspicious activity

- Always report any suspicious activity to IT. Part of our job is to stop cyber attacks and to make sure our data isn't lost or stolen
- All of our jobs depend on keeping our information safe
- In case something goes wrong, the faster we know about it, the faster we can deal with it

Security threats are here to stay and changing constantly over time. But by following this tip and others in your IT security employee handbook you won't accidentally put yourself and our business in a compromised position.

Take care and stay safe.
[Your name]

IT Security DOs and DON'Ts
what to do | what not to do | what to look out for

IT Security Dos and Don'ts
Courtesy of RMON Networks
rmonnetworks.com
603-642-4010

RMON
NETWORKS



We have some samples here of what is in our training kit. You can use this as a starting point. Change, or add what ever you'd like.

State of NH Resources

Ransom Note

NH Dept. of
Information
Technology

[https://www.nh.gov/
doit/cybersecurity/in
dex.htm](https://www.nh.gov/doit/cybersecurity/index.htm)

NH Dept. of
Homeland Security
and Emergency
Management

[https://www.nh.gov/
safety/divisions/hse
m/contactus.html](https://www.nh.gov/safety/divisions/hsem/contactus.html)



Malware Wears Costumes, Too

October 2013
Volume 10, Issue 10



NH Department of Information Technology
www.nh.gov/doit/cybersecurity

October is not only National Cyber Security Awareness Month, it's also the time to celebrate Halloween, a time of fun, candy, and costumes. Much like trick-or-treaters and other Halloween mischief makers, malware can use 'costumes' to disguise what it is and to trick you into installing it. These 'costumes' come in many forms but if you know what to look for, you can avoid the tricks.

Trojan Horses

Trojan Horses are a type of malware that misrepresent themselves to look legitimate, much like the Trojan Horse the Greek army used to enter Troy. Trojan Horses may be apps in smartphone stores, freeware and shareware, or even attachments to emails. The last is a very common spam technique and is often used with spam email campaigns that say you have a voicemail, fax, or shipping notification. When you click the attached document to hear the voicemail, or see the fax or who has shipped you a package, the file opens to show you what you expect to see or hear, but in the background malware is downloading on to your computer.

Drive-by Downloads and Malvertising

Drive-by downloads occur when a program is downloaded onto your device without your permission. One way this happens is through malicious advertising or *malvertising*. You know the advertisements that appear on the edge of many webpages? When malicious actors purchase advertising space there, they can install malware in the advertisement. That means that if you see that malicious advertisement, which looks like any legitimate advertise, the malware hidden in the advertisement will automatically try to download onto your device.

Social Engineering - Malicious Links

Social engineering relies on tricking you into taking an action, such as clicking on a link. As the malicious website opens, malware can be installed on your device. Simply visiting these websites is enough to infect your device.

The NH Department of Information Technology has great information that you can share with employees for awareness training! These would be great article to share once or twice a month!

FTC is another great resource for information as well. These will all help you build programs.


Ransom Note

Are there tools that businesses can employ that will warn if their data is about to be encrypted?




Ransom Note

Chris Chaves,
Senior Security
Engineer,
Sophos



SOPHOS



Thank you David. And now we are going to turn over the presentation to Chris Chaves from Sophos. Sophos is a leader in the security industry, and one of our trusted partners. Chris is here to discuss their revolutionary new product called Intercept X. We just discussed a key component to preventing ransomware is utilizing all of the features your endpoint has available. InterceptX is additional layer for Endpoint Security, and it was just released mid – September, and it can actually STOP ransomware! This is really exciting, I think the technical folks on the line will really appreciate this portion of the presentation. Welcome Chris Chaves.

Endpoint Security has reached a Tipping Point

- *Attacks are from within the perimeter, delivered using Software Exploits*
- *Ransomware reaches \$1.2B in damages*
- *Lack of Threat Intelligence after a Breach*

NHMA

Setting the scene – why do we need InterceptX

Attacks are focused on the endpoint, evading traditional perimeter defenses, using software exploits to deliver malicious payloads

90 % of breaches are from software exploits – NSS Labs

90+ % of exploits are from known vulnerabilities – ie: non zero day, patches available

66 % of IT staff lack incident response skills (Sans Survey into Incident Response)

The next generation of security - Sophos Intercept X

Anti-Ransomware	Root-Cause Analysis	Anti-Exploit
Detect Next-Gen Threats <ul style="list-style-type: none"> Stops Malicious Encryption Behavior Based Conviction Automatically Reverts Affected Files Identifies source of Attack 	Automated Incident Response <ul style="list-style-type: none"> IT Friendly Incident Response Process Threat Chain Visualization Prescriptive Remediation Guidance Advanced Malware Clean 	Prevent Exploit Techniques <ul style="list-style-type: none"> Signatureless Exploit Prevention Protects Patient-Zero / Zero-Day Blocks Memory-Resident Attacks Tiny Footprint & Low False Positives
Prevent Ransomware Attacks Roll-Back Changes Attack Chain Analysis	Faster Incident Response Root-Cause Visualization Forensic Strength Clean	No User/Performance Impact No File Scanning No Signatures

Ransom Note

NHMA

ADVANCED MALWARE

LIMITED VISIBILITY

ZERO DAY EXPLOITS

The existence of advance malware such as crypto-ransomware variants presents a very visible problem.

Yet IT and security teams have limited visibility in to the threats hitting their endpoints today.

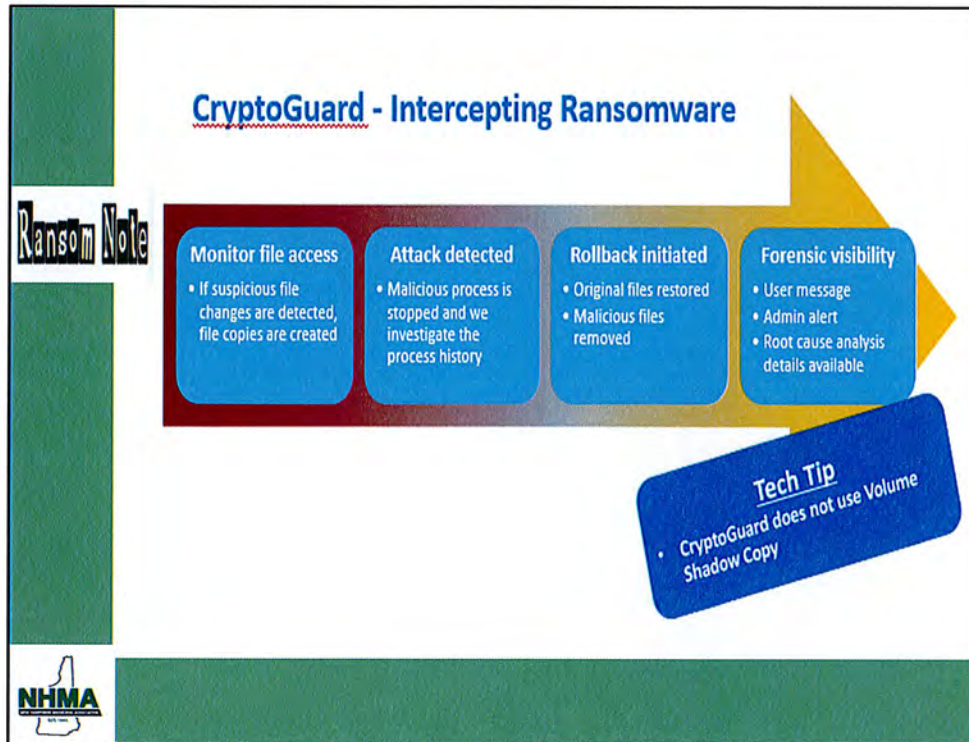
And the software we use daily is being turned against us – the number of software vulnerabilities being recorded is increasing, we have to patch and patch fast – but patching is like closing the stable door after the horse has bolted.

Enter the next-generation – a completely new approach to endpoint security

Ransom Note

ANTI-RANSOMWARE





Monitor for distinct changes in the file headers




Ransom Note


ROOT CAUSE ANALYSIS



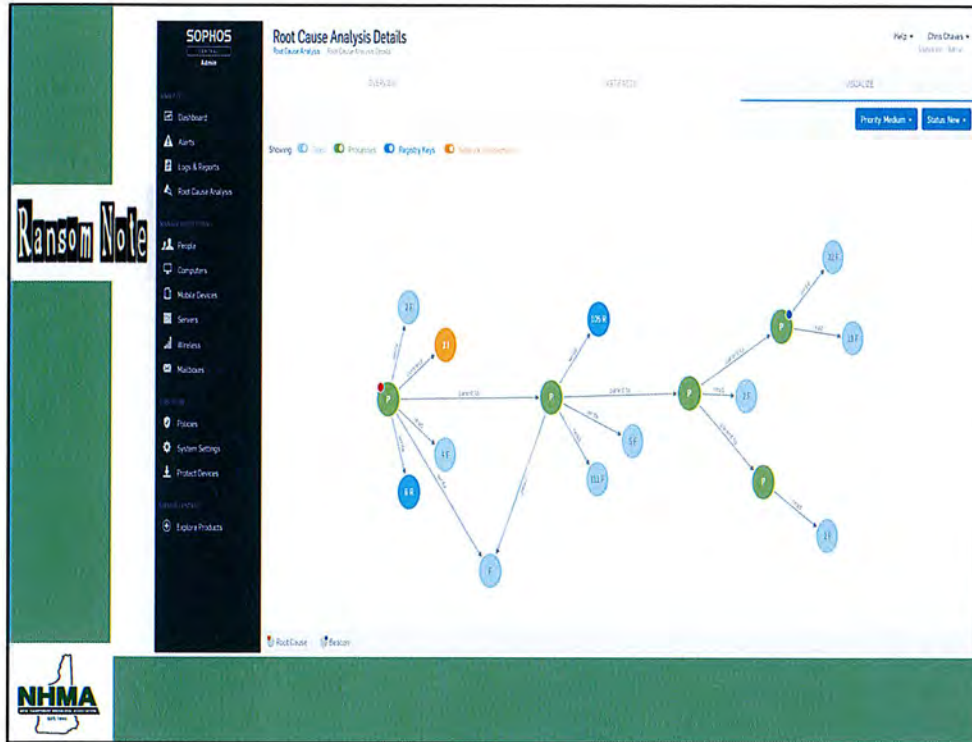
Root-Cause Analytics

Understanding the Who, What, When, Where, Why and How

What Happened?	<ul style="list-style-type: none"> ▪ Root Cause Analysis <ul style="list-style-type: none"> ▪ Automatic report @ the process / threat / registry level ▪ 90 Days of historical reporting ▪ Detailed Visual representation of what other assets have been touched 	
What is at Risk?	<ul style="list-style-type: none"> ▪ Compromised Assets <ul style="list-style-type: none"> ▪ Comprehensive list of business documents, executables, libraries and files ▪ Any adjacent device (i.e., mobile) or network resources which may be at risk 	
Future Prevention	<ul style="list-style-type: none"> ▪ Security Posture <ul style="list-style-type: none"> ▪ Recommendations based on historical security risks ▪ Provides steps to prevent future attacks ▪ Rich reporting of Compliance status 	



Monitor for distinct changes in the file headers



Our Incident Response engine automatically capture core data on an incident. Showing crisp summary data and details a human can understand. PLUS IT people can add comments and actions to each incident as its investigated. We AUTOMATICALLY add a priority depending on our analysis of the root cause and the chain itself. Obviously someone can add to this, for example here is a piece of ransomware attempting to start encrypting your business files.

SOPHOS
UKLT0345
Computers (1/1)

SUMMARY **EVENTS** **STATUS** **POLICES**

Recent Events [View More](#)

- ⊘ CryptoGuard detected ransomware in C:\Windows\System32\crypt.exe Sep 1, 2016 11:39:50 AM
- ⊘ Update succeeded Sep 1, 2016 11:37:27 AM
- ⊘ Robot recommended after software update Sep 1, 2016 11:28:25 AM
- ⊘ Peripheral allowed: NEC/Mitsumi SATA/CD/DVD/ATA Device Sep 1, 2016 11:17:33 AM
- ⊘ Robot recommended after software update Sep 1, 2016 11:17:29 AM

Show Status

OS: Windows 7 (64-bit)
IP: 10.10.10.10
Location: Desk
Device: Desktop

Endpoint Agent Summary

Last Activity: 4 minutes ago [Scan Now](#)

Agent Update Status: 10/10/2016 11:00 Update Successful ✓

Tamper Protection

Tamper Protection: On - Disable Tamper Protection [View Details](#)

NHMA

Intercepting Exploits

Ransom Note

The slide features a background image of a computer screen displaying a list of exploit techniques. A central white text box is overlaid on the screen.

Malware techniques
10's of new malware sub-techniques every year
100,000,000+

TECHNIQUE DESCRIPTION

- Stack Pivot**
Force the stack to have address memory of 0x00000000
- Stack Pivot**
Force the stack execution to 0x00000000
- Kernel**
Not Callable to interrupt disabled by system hardware
- Heap Spraying 1**
Write calculated hex strings to heap
- Heap Spraying 2**
Write calculated hex strings to heap
- Shellcode**
Write shellcode to memory
- Lockdown 1**
Control program flow
- Lockdown 2**
Control program flow

Exploit Prevention

- Monitors processes for attempted use of exploit techniques e.g Buffer overflow, code injection, stack pivot and others
- Blocks when technique is attempted
- Malware is prevented from leveraging vulnerabilities



Most popular exploit payload – Ransomware.



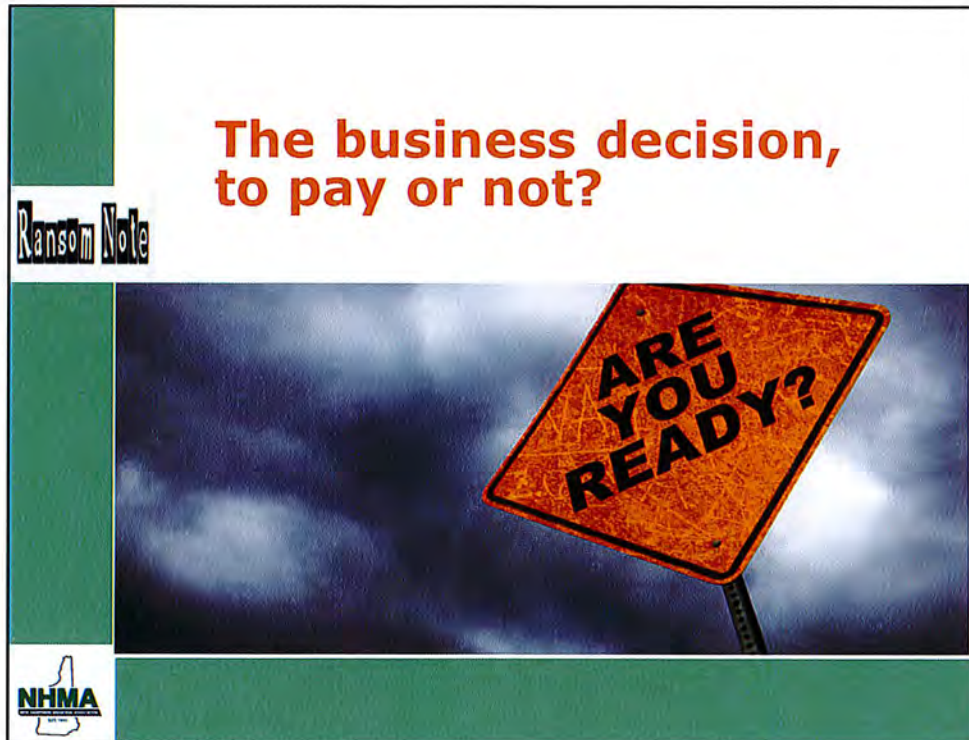
Only by adding Intercept X on top of Endpoint Advanced do you truly build, complete next generation endpoint detection and response capabilities.

You can choose to build your own by layering intercept x on top of their chosen endpoint – adding anti-exploit, anti-ransomware and greater visibility to your current suite.

Ransom Note

**If you fall prey
to ransomware,
should you pay?**



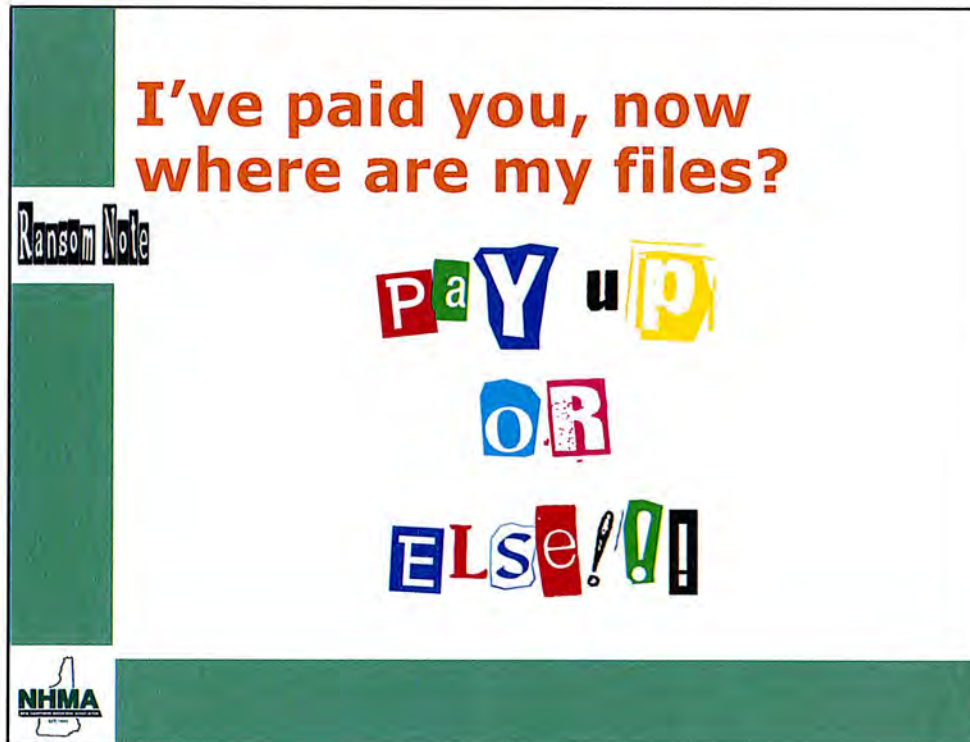


This is a business question is totally up to you. Obviously you do not want to have to pay and encourage the bad guys. Sometimes people have to. There are a lot of unreported cases because people are embarrassed. If you work at a company you should absolutely tell your IT Department because they hopefully have a backup.

There is going to come a day when this will become more than about money. Criminals may someday ask you to steal confidential business data.

With the internet of thing just consider what the future of ransomware could be. Need to get to work? Pay me, or I won't start your car. It's freezing outside, don't want your pipes to freeze, pay me or you won't have access to your thermostat controller.

So, be prepared, and don't pay if you don't have to.



Ransomware has built a trustworthy reputation for itself. Victims have paid the ransom, and then they get their files back.

However, if you have a bit of experience with ransomware, then you know this is not always true.

- Something could go wrong in the decryption process.
- The hacker could decide he wants more money.
- Your files could get re-encrypted all over again, if you don't properly remove the virus.

In the case of Greenland, NH the information did not make it to the town administrator in time, and it was just too late!

The point is... Cyber criminals really cannot be trusted, despite the image they have created.

We really hope it never has to come to this point for you. That is why we are here today educating you on the prevention methods for not only your systems, but users too.

Do something before you become a statistic!

Ransom Note

- Medfield, MA
 - Paid the ransom
- Tewksbury, MA Police Dept.
 - Paid the Ransom
- Durham, NH
 - Utilized Backups
- Greenland, NH
 - Lost 8 YEARS of data!



This information is only what is in the Media! Trust me, there are many other stories that are not being reported. There are stories from towns we have spoken with each year at the annual conference that were nearly as bad as the Greenland!

When you think about the type of information that state and local agencies hold, like resident's tax information, property information, social security numbers, birth and death certificates and emergency contact information, we really hope that people don't have to learn the hard way when it comes to ransomware.

Q & A with the experts

Ransom Note



Chris Chaves
Senior Security Engineer
Sophos



David Cohen
Senior Security Engineer
RMON Networks

AVAILABLE RESOURCES:

- Download your FREE, fully editable Employee Training Kit.
- Start your 30 Free Trial of Intercept X

BOTH AVAILABLE AT:

[www.rmonnetworks.com/
InformationSecurity](http://www.rmonnetworks.com/InformationSecurity)



This information is only what is in the Media! Trust me, there are many other stories that are not being reported. There are stories from towns we have spoken with each year at the annual conference that were nearly as bad as the Greenland!

When you think about the type of information that state and local agencies hold, like resident's tax information, property information, social security numbers, birth and death certificates and emergency contact information, we really hope that people don't have to learn the hard way when it comes to ransomware.





Right-to-Know Law: Current Issues

Wednesday, December 7, 2016

6:00 p.m.— 8:00 p.m.

NHMA Offices, 25 Triangle Park Drive, Concord

The Right-to-Know Law affects every aspect of local government in our state. Every board, committee, commission, and sub-committee in every town, city, and village district in New Hampshire must comply with this law. As a result, all local officials and employees should be aware of the law and what their responsibilities are regarding both public meetings and governmental records.

This free session is open to all local officials from NHMA member municipalities. NHMA staff will provide an overview of the law and address some of the most difficult issues under the law, including confidential information, electronic records and communication, procedures for non-public session, and communications outside a meeting. There will be ample time for questions and answers on all aspects of the law.

Register online at www.nhmunicipal.org under CALENDAR OF EVENTS



Questions? Please call 800.852.3356, ext. 3350 or email NHMAregistrations@nhmunicipal.org



Visit NHMA's Anniversary Webpage:
www.nhmunicipal.org/anniversary





*for attending
our webinar
presentation
today!*

Mission Statement

The New Hampshire Municipal Association non-profit, non-partisan association working strengthen New Hampshire cities and towns their ability to serve the public as a member-funded, member-governed and member-association since 1941. We serve as a resource information, education and legal services. NHMA is a strong, clear voice advocating for New Hampshire municipal interests.

25 Triangle Park Drive
Concord, NH 03301
www.nhmunicipal.org or
legalinquiries@nhmunicipal.org
603.224.7447
NH Toll Free: 800.852.3358

