Subject: **[Cag-iaad] [Hod-list] Alert on Petya/NoPetya Virus**
To: cag-iaad@lsmgr.nic.in

Date: 06/28/17 01:44 PM
From: Sanjay Kumar <aao3is@cag.gov.in>
Sender: cag-iaad-bounces@lsmgr.nic.in

ransomware.pdf (162kB)

Dear Sir/Madam

This has a reference of recent attack on IT System & Applications. The NIC has sent an Advisory on virus Attacks and the same is being sent to your office for information and necessary action at your end.

Regards

AAO(IS)

-------- Original Message --------
From: **Rajasekhar K** <head-cdg@gov.in>
Date: Jun 28, 2017 9:49:22 AM
Subject: [Hod-list] Alert on Petya/NoPetya Virus
To: hog-list@lsmgr.nic.in, sio-list@lsmgr.nic.in, hod-list@nic.in
Subject : Alert on Petya/NoPetya Virus .

1.What is Petya/NoPetya ?
It is a new ransomware virus. It is not similar to Petya virus as thought initially. So It is being called NoPetya.

2.In what way it is different from Wannacry ?

NoPetya virus is deadlier than Wannacry. Wannacry has several bugs and used to encrypt the files and its spread vectors are limited. Petya/NoPetya not only encrypts it also modifies the files and uses the infected systems to attack other systems. NoPetya is developed by professionals. It can attack even patched computers also.

3.How it spreads ?
It spread via multiple channels – such as emails un-patched systems and then other nodes on the network.

Besides old Windows XP systems it can affect Windows 10 systems also [due to the EternalBlue vulnerability MS17-010].

The NoPetya ransomware can detect and extract passwords from memory or from the local filesystem of the infected computers to spread to other computers in the network.

After spreading it may use the tool PsExec to execute malicious code on other computers .In this way it spreads much faster than Wannacry.

If the infected system has administrator access to the network, then virus can spread the entire network.

Even a single un-patched weak computer is enough to get attacked easily and spread the attack vector across the network to even other patched nodes of the network.

4.What is its impact so far ?

So far the systems in 2000 organisations across the Globe located in Ukraine, Russia, the U.K other EU countries and the United States were attacked.
Big Concern - RAAS (RAnswomware As Service) the creators of NoPetya offer it as a service over darknet, for 15% commission, so distributors get a share of 85% of the cybercrime booty.
So far 22 payments worth US$5,515 were paid to 2.39818893 Bitcoin.

5.How to protect and prevent the attack ?

All the guidelines issued in the earlier advisory can help securing and safeguarding their digital data and assets. The advisory is attached herewith for ready reference.

K Rajasekhar
Dy Director General & HoG
NIC Centre for Data Governance.
MeitY, Govt of India.

--
With Regards

Jaskaran Singh Modi
Technical Director

Audit Informatics Division,O/o Comptroller and Auditor General of India , Bahadur Shah Zafar Marg,New Delhi -110002
Mobile :+919582944787,IP Phone : 65001 Direct :011-23236080

NIC Advisory on Ransomware Attacks.

A. What is a ransomware attack?

Attacks involve malware delivered through spear phishing emails that lock up valuable data assets and demand a ransom to release them.

Hackers now check a victim's social media accounts, and create a fake email address pretending to be a friend or contact in order to get them to click on an infected link or attachment.

"It's much more targeted, and will exploit a particular vulnerability in a device, application, server or software,

The Health / Education / social sector is highly targeted by hacker attacks, due to antiquated or misconfigured computer security systems and the amount of sensitive data they hold.

B. How to Prevent Ransomware Attacks ?

1. Do not click hyper links from un-known sources, and without establishing authenticity of link even from known sources.
2. Prepare a up-to-date inventory of all the “Digital Assets” at various locations/facilities being used by the various functionaries of the organization.
3. Make a trustworthy knowledgeable functionary (permanent Government employee) Administrator of the Digital Assets (ADA) of the organization at each location.
4. Let ADA keep all software (especially the system software) up to date, including operating systems and applications.
5. ADA has to ensure back-up of all digital content located in the digital assets under ADA jurisdiction every day, including information on employee devices, so ADA can restore encrypted data if attacked by ransomware.
6. Back up all digital content to a secure, offsite secret location(s) within organization.
7. Distribute Back-up : Divide the digital assets and distribute the back-up locations. Don't place all data on one back-up file and share it.
8. ADA in collaboration with NIC officials, to train all the staff using the digital assets including mobile devices connected to network, on cyber security practices, emphasizing not opening attachments or links from unknown sources.
9. Develop a communication channel and strategy to quickly inform all employees if a virus reaches the company network.
10. If every bit of data of the organization is safeguarded and back-up is kept secretly, even if hackers attack and demand ransom, Govt can launch an investigation rather than making payment.
11. Mandate security auditing by ICERT empanelled auditors for all the digital assets as per GoI policy.

12. ADAs in collaboration with information security teams of ITE&C Dept and NIC to perform penetration testing to detect the vulnerabilities.
13. Register all the devices and digital assets. Strictly avoid usage of un-registered and un-monitored devices.
14. Adopt and use standard security and data privacy policies as per advisories from ITE&C Dept, NIC/ Govt of India.
15. Ensure all devices and systems are protected well with latest firewalls and anti-virus systems.

C. Mitigating an attack

1. Remove the infected machines from the network, so the ransomware does not use the machine to spread throughout your network.
2. Report the attack and register all information related to attack.
3. Facilitate investigation of the attack.
4. Let one authorized spokesperson of the entire department only communicate with media the information related to attack.
5. A inventory of attacks and decryption kits / mitigation kits to be maintained.

Subject: **[Cag-iaad] [Hod-list] Petya Ransomware variant – Advisory for the users**
To: cag-iaad@lsmgr.nic.in

Date: 06/28/17 04:57 PM
From: Sanjay Kumar <aao3is@cag.gov.in>
Sender: cag-iaad-bounces@lsmgr.nic.in

Dear Sir/Madam,

This is in continuation of email dated 28.06.2017 forwarding therewith Advisory on virus Attacks.

As a preventive measures and for remedial action, NIC has now forwarded us Advisory for users. This may kindly be accord immediate attention and to take preventive measures as suggested by NIC.

-------- Original Message --------
From: **Ravi Vijayvargiya** <ravi.vijay@nic.in>
Date: Jun 28, 2017 12:23:47 PM
Subject: [Hod-list] Petya Ransomware variant – Advisory for the users
To: hog-list@nic.in, hod-list@nic.in, sio-list@nic.in
Cc: pradhan@nic.in, dg@nic.in, neeta@nic.in, csg-list@lsmgr.nic.in

This issues with the approval of HOG Cyber Security

Petya Ransomware variant – Advisory for the users

A variant of Petya ransomware is spreading across the globe. For protecting systems in NICNET the following actions need to be taken to control the spread of the Petya Ransomware:

1. Users are advised not to open any unknown mails containing attachments with the following extensions (currently known as being affected):

.3ds, .7z, .accdb, .ai, .asp, .aspx, .avhd, .back, .bak, .c, .cfg, .conf, .cpp, .cs, .ctl, .dbf, .disk, .djvu, .doc, .docx, .dwg, .eml, .fdb, .gz, .h, .hdd, .kdbx, .mail, .mdb, .msg, .nrg, .ora, .ost, .ova, .ovf, .pdf, .php, .pmf, .ppt, .pptx, .pst, .pvi, .py, .pyc, .rar, .rtf, .sln, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls, .xlsx, .xvd, .zip

2. Do not click any links of email content which may lead to download of the ransomware.

3. The three centrally managed antivirus solutions namely TrendMicro, Symantec and McAfee deployed in NICNET have the required signatures to protect against this ransomware. Ensure up-to-date antivirus signatures.

4. Ensure up-to-date Operating System patches.

5. The propagation method appears to be via the Remote Desktop Protocol (RDP) and/or Server Message Block (SMB) protocols. Advised to avoid / minimize the use of these protocols.

Regards

Ravi Vijayvargiya

Sr. Technical Director & HoD, Network Security Division, NIC(Hq), N. Delhi

Contacts: +91-11-24305122, 24365123, 9911378797 *ravi.vijay@nic.in*

--
With Regards

Jaskaran Singh Modi
Technical Director

Audit Informatics Division,O/o Comptroller and Auditor General of India , Bahadur Shah Zafar Marg,New Delhi -110002
Mobile :+919582944787,IP Phone : 65001 Direct :011-23236080
