‘WannaCry’ ransomware attack

EY response to the global cybersecurity incident May 2017

Executive summary

On 12 May 2017, a global ransomware attack occurred across a wide range of sectors, including health care, government, telecommunications and gas, spreading to over 230,000 systems in over 150 countries. Ransomware isn’t new – over the last five years the number of ransomware attacks has grown tremendously, usually with financially motivated cyber criminals extorting relatively small amounts of money from victims whose data they are holding hostage. The criminals promise that payment will result in data being released, but this does not always happen. This attack differs in that it is the first time ransomware has been used in conjunction with self-propagating malware (commonly known as “worms”), enabling it to spread more aggressively to other computers over an organization’s network without requiring further interaction from users.

Although WannaCry reportedly stopped actively spreading on Sunday 14 May, after the “kill switch” was activated, EY has seen reports of new variants being released that do not contain a kill-switch built in to stop it from spreading. As yet there is no clarity on the perpetrators, only rumors.

Why is this attack significant?

The global scale and what appears to be indiscriminate targeting of organizations emphasizes the need for all companies to pay attention to security basics, such as: keep systems up-to-date with software patches, make regular backups of data and educate users not to click on suspicious links.

The cost of the operational disruption has been significant overall, but variable by sector and organization. The actual cost to organizations is not yet known, and will differ for every victim. The instigators may not receive much in ransom payments at all – currently only around $50,000. The likelihood of identifying the culprits appears to be fairly low and the process of bringing them to justice would be long and costly. This is likely to be of little consolation to the many organizations who will suffer costs and data loss arising from this cybercriminal activity, or for those who paid an indirect price, such as their hospital operation being cancelled.

Further context

The WannaCry incident highlights the need for organizations to get the cybersecurity basics right. These include:

- **First:** identify and manage the organization's cyber risks — with a specific focus on the priority cyber threats and breach scenarios that could disrupt operations or have other negative impacts on the organization.
- **Second:** continually educate the organization's employees in good cybersecurity practices and the use of third-party assessment/assurance programs.
- **Third:** maintain awareness of the cyber threat environment to the organization. Cyber criminals and other attackers are constantly evolving their methods to create ever-more effective ways of exploiting vulnerabilities for monetary gain or disruption purposes — often this involves interfering with data integrity rather than compromising its confidentiality.
- **Finally:** maintaining and regularly reviewing elements of a cybersecurity program. Doing so will help provide a strong foundation for building cyber resilience into your organization — patch often, define your cyber incident response process, back up regularly and practice response scenarios.

  There are a number of existing technical references that provide further guidance:

  - https://www.us-cert.gov/ncas/alerts/TA17-132A
    http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
  - http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=d4d15d30-e775-4f6f-b838-d3caca05a5e9

Contact information

General inquiry — EMEA

Paul Walker
Partner, EY (UKI & EMEIA) LLP
+44 7958 766 666
pwalker@uk.ey.com

Owen Purcell
Partner, EY (UKI) LLP
+44 207 951 0059
opurcell@uk.ey.com

Example

- Visible message is displayed on the users machine with the following "Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted. If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely! Let's start decrypting!"

Additional Information

- Microsoft, in an unusual move, released a patch for the underlying Server Message Block (SMB) vulnerability for Windows XP and older versions, which they officially no longer support with "free" security updates. They did this to help prevent spreading of this attack and reduce overall vulnerabilities.
- The vector used by WannaCry allows the ransomware infection to spread from computer to computer inside a network and without user interaction by leveraging a previously identified exploit in Windows SMB.
- Users impacted by the WannaCry ransomware are reporting being locked out of systems with instructions displayed for the payment of $300-$600 via bitcoin to release files that will otherwise remain permanently encrypted.
- The tool and the language used in the instructions have been translated into multiple languages demonstrating a coordinated and well-constructed approach to gain maximum impact.

Remediating the issue

Preventive measures to reduce the risk of ransomware

EY member firms range of cybersecurity services, including proactive penetration testing, Cyber Transformation and Managed Security Operations centers, can be leveraged to prevent a ransomware outbreak within an organization. Through these services the following activities are recommended:

- Ensure vulnerability and patch management policies and procedures are up to date across the estate and are implemented through appropriate change control procedures. Where out-of-date and legacy operating systems are used, seek guidance from vendors on further steps.
- Maintain an effective enterprise incident response and business continuity plan that is tested and measured for effectiveness against ransomware and other potential attack methods, as well as updated to reflect the current cyber threat environment.
- Ensure the organization has a security awareness training program in place with proactive testing, including screenshots of what to look out for. Clear guidance should be provided on the immediate steps alongside incident reporting guidelines. This should be communicated to all users and third parties who connect to the organization's network.
- Organizations must ensure regular, tested backups are in place to mitigate effects of possible infection and speed the recovery process in lieu of succumbing to ransom payment demands.
- Seek assurance from third parties who connect to your network that they are following similar actions to yourself and that they are appropriately protecting themselves.
- Implement endpoint monitoring, giving security operations teams the visibility into malicious behavior occurring in the environment.
- Identify critical systems and data and confirm these are connected to the internet only when necessary.
- Make sure to test the security program with frequent penetration tests across the estate.
- Review how proactive security monitoring of the entire environment through EY Managed SOC services could enable faster detection and response to incidents.

Business response and forward look

If an organization believes it is compromised, or is in the process of being compromised then the following activities can help to provide a rapid response, damage containment and communications to end users:

- Disconnect infected machines from the network and take all backups offline. These could become encrypted as well if left connected to the network.
- EY member firms FIDS Forensic Technology & Discovery services team can be used to:
  - Forensically analyze network and host systems to detect early indications of penetration by ransomware to allow more rapid response and remediation.
  - Forensically detect, identify and contain ransomware malware based on previous experience with ransomware negotiations and ransomware eradication. Forensically circumvent ransomware and/or recover data from damaged systems and/or backups, and verify that recovered data are clean from ransomware contamination.
  - Forensically image and preserve highly sensitive impacted machines to support the systems and data are not destroyed by ransomware.
  - Collect and preserve IT and business evidence in a forensically sound manner, and then provide internal or stakeholder investigations and support disputes with customers, service providers and requirements for regulatory reporting.
- Activate your incident response plan and don't treat the investigation as merely an IT issue; there should be cross-functional representation in the investigation team such as: legal, compliance, information security, business, PR, HR, etc.
- Identify and address vulnerabilities in the environment, sufficiently harden the environment to complicate the attacker's effort to get back in, enhance the ability to detect and respond to future attacks and prepare for eradication events.
- Activate your business continuity plan. Prepare data based on varying requirements for regulatory inquiries or civil suits.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 03261-173Gbl

ey.com/cybersecurity
ey.com/ransomware