RAMPANT RANSOMWARE

WanaCrypt0r incident response and how to avoid future attacks

Accenture Security

STATE OF THE HACK:
WANACRYPTOR

Organizations around the world face an increasing risk from diverse and ever-evolving cyber threats. Ransomware, also known as cryptoware, attacks a company's data by encrypting it until a ransom is paid—with no guarantees that the data will be decrypted once the payment has been made to the adversary. Threat intelligence and law enforcement agencies that work with Accenture warn such attacks are accelerating in frequency and targeting more businesses with increasing ransom demands. The latest in such attacks is WannaCry, also known as WanaCrypt0r.

According to multiple sources, on May 12, 2017, around 4 a.m. ET, security researchers and various organizations started reporting a widespread ransomware campaign targeting multiple organizations and affecting countries across the globe. The malware, dubbed WanaCrypt0r, had been spreading rapidly that day, causing disruption in more than 160 countries. The malware requested a ransom in bitcoins of a value ranging from US$300 to US$600 per infected computer.

By continuously conducting intelligence collection and research operations on major phishing campaigns as well as other malware families and their associated adversaries, the Accenture Security iDefense Threat Intelligence team had already identified five out of the six initial infrastructure nodes used by WanaCrypt0r. iDefense observed a considerable amount of crimeware, sharing similar infrastructure to WanaCrypt0r. In this case, iDefense observed the sample uses specific TOR exit nodes through a pre-determined list of nodes that were also used in previous ransomware attacks. *Through its intelligence feeds, iDefense clients already had protection against some of the initial threat infrastructure leveraged in this attack as early as March 8, 2017.* Further to this, clients utilizing our Cyber Defense services such as Incident Response and Threat Hunting with Endgame End-point Detection and Response (EDR) Integration, were also protected prior to the proliferation of this threat thanks to Endgame's behavioral analytics and machine-learning engine.

Infection statistics

MORE THAN
90,000
INFECTED SYSTEMS

PRIMARILY AFFECTED
HEALTH AND TELECOMMUNICATIONS
CLIENTS[1]

MORE THAN
160
COUNTRIES AFFECTED

Affected countries: Russia, China, Taiwan, Ukraine, United States, Canada, South Korea, France, India, Brazil, Hong Kong, Japan, England, Germany, Poland, Chile, Mexico, Spain and Italy.

Current assessment

Customers should consider this attack to have a potentially EXTREME impact on their organization, if affected, as it can disrupt the operations of any enterprise. Although the initial observed variant of WanaCrypt0r's "kill switch" domain has been sinkholed, we still consider the malware to be a major threat due to the likelihood of new variants emerging in the coming days and the apparent lack of effective patching and other controls within targeted organizations.

Additionally, we assess that other threat actors will likely attempt to leverage the same vulnerabilities to attack other organizations with more robust future variants.

Technical details

Initial reports claimed that the malware was delivered through phishing campaigns; however, no security vendor or affected organizations were able to definitively identify such e-mails as the attack vector. The security community identified only a handful of e-mails, but it was determined that these e-mails were delivering a different malware family.

Further research revealed that attackers likely leveraged a critical SMB vulnerability on Windows operating systems. Microsoft Corp. had released a security update for the MS17-010 vulnerability on March 14, 2017; however, unpatched systems with direct access to the Internet were likely exploited and were the initial infection vector in each affected organization.

[1] *The initial infected entities were the UK National Health Service (NHS), and Telefonica de Espana.*

WanaCryptOr's main characteristics

Use of a kill switch to determine whether to encrypt files on an infected system. The kill switch is a simple URL check request. While it was "activated" on March 12, if a system is unable to reach the URL (due to proxy or otherwise), it will result in file encryption

Use of asymmetric encryption with the creation of a random set of public/private keys for each infected computer

Ability to delete shadow copies and modify Windows boot menu to ignore errors

Worm capability using windows file sharing resources (including IPC) to spread laterally on a network

Ability to exploit SMB vulnerabilities described under advisory MS17-010 (ETERNALBLUE – CVE-2017-0145)

Ability to exploit users Remote Desktop Protocol (RDP) sessions

Use of ransom notices in 27 languages

Use of TOR clients

Requested payment in bitcoins

Protection against WanaCrypt0r

Accenture Security recommends performing the following actions to help protect an organization against the WanaCrypt0r ransomware:

- Implement proper patch management practices, to rapidly evaluate and deploy security updates, with priority given to applying the patch for the vulnerability exploited by WanaCrypt0r (MS17-010)
- Impose a strict policy preventing access to shared network resources from personal laptops
- Monitor, but do not block, traffic to the following kill-switch websites:
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea <.> com
  - ifferfsodp9ifjaposdfjhgosurijfaewrwergwea <.> com
- Disable SMBv1 wherever possible
- Disallow inbound/outbound SMB or RDP connections to/from untrusted networks
- Keep anti-virus products and endpoint solutions fully up-to-date and integrated with timely threat intelligence
- Maintain regular and robust backups of storage devices, servers, and end-users' computer data
- Block network traffic to TOR, peer-to-peer, and other similar services unless allowing such traffic is a business requirement
- In case of infection or detection, immediately disconnect affected systems from the network
- Reimage infected systems (capturing a forensic image if appropriate), whenever possible, and restore a user's data from a backup copy, taking special care to find the initial infection, to avoid re-infecting systems

Security first

Although the nature of the recent cyber attack was not unexpected, its scale, in terms of the number of countries and organizations affected, is unprecedented. As a result, due to the critical impact it has had on the operations of many organizations, the attack has been identified as "extreme" malware. There is no time to lose in taking the appropriate steps to not only recover from the incident, but also protect against similar threats or variants, and, ultimately, to better keep organizations safe in the likely event of future ransomware attacks.

The Accenture Security iDefense Threat Intelligence team covered a new cyber crime dynamic in its 2016 Cyber-threats and Trends report: ransomware-as-a-service (RaaS). Malicious actors packaged successful variants of extortive malware into kits that could enable less-skilled malicious actors to employ this threat tactic with little effort or technical knowledge.

In the first half of 2016, there were widespread reports on the Internet of new ransomware variants and ransomware infections affecting various organizations across a wide swath of industries in both the public and private sectors. One well-publicized report concerned the Hollywood Presbyterian Medical Center ransomware infection from February 2016. In addition to turning away ambulances, hospital staff were forced to manually write down patient information because they had no access to computers, and eventually, the hospital declared an internal state of emergency.

Fast forward to today, and the cyber attack scenario is being repeated across the National Health Service in the United Kingdom and many other organizations globally. Ransomware is not new but the size of this attack by the WannaCry malware is “unprecedented”, according to European Union police body Europol.

To help reduce the chances of falling victim to a ransomware attack, we would like to share the following practices that leading companies have taken to protect themselves.

PHISHING ATTACKS

Most ransomware attacks originate as a phishing attack. Prevention training and awareness programs can help employees recognize telltale signs of phishing scams and how to handle them. **Leading programs typically include:**

Training to help employees recognize and avoid fraudulent e-mails.

Guidance on how to respond if an employee believes he or she is victim of a social engineering attack.

Frequent tests that assess employees' adoption of the guidance provided.

RANDSOMWARE AND E-MAIL CONTROLS

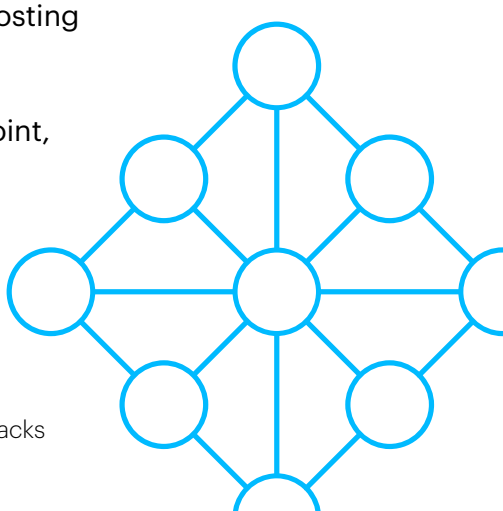
Ransomware attacks are frequently delivered via e-mail. Strengthening e-mail controls can often prevent malicious e-mails from reaching employees. **Consider taking the following steps to protect e-mail environments:**

- Enable strong spam filters to prevent suspicious e-mails from reaching end users.
- Authenticate inbound e-mail using Sender Policy Framework and Domain Keys Identified Mail to prevent spoofing.
- Scan incoming and outgoing e-mails to detect threats and filter executable files.
- Deploy a cloud-based e-mail analytics solution such as Proofpoint or Microsoft ATP to identify and quarantine known threats distributed via malicious e-mail.
- Configure e-mail in a manner that clearly identifies external e-mail as originating from outside the enterprise, prompting employees to be more cautious.
- Display file extensions, making it is easier to spot file types not commonly sent to employees, such as JavaScript.
- Consider installing the Microsoft Office viewers that do not support macros to enable employees to see document content without opening the document.

PROTECTING INFRASTRUCTURE

Attackers are getting smarter and unsuspecting employees can make mistakes and fail to recognize malicious e-mails. **In these cases, the following actions could be considered to help protect your infrastructure:**

- Remove or limit local workstation admin rights.
- Use endpoint protection that includes heuristic behavior analysis and updates signatures frequently.
- Maintain a workstation security compliance program to validate that all relevant tools are in place and working.
- Segment networks so servers and workstations are not in the same network.
- Review security systems for appropriate configurations/hardening (virus scanners, firewalls, intrusion prevention systems, e-mail/Web gateways).
- Set default execution commands to 'no.' This helps keep servers secure by identifying authorized applications and limiting what each can change and update. It also prevents attempts to make changes that block ransomware from contacting command and control servers and downloading malicious software.
- Regularly patch operating systems and applications so that known vulnerabilities are not exploited.
- Limit administrator access to only those "in need."
- Configure security, information and event management (SIEM) solutions to flag incidents and enable automated cleanup methods.
- Implement and/or tighten Web filters/URL blockers. Along with clicking on links within phishing e-mails, employees introduce malware by visiting compromised webpages. Web filtering helps block websites hosting ransomware, as well as their command and control servers.
- Deploy a cloud-based analytics tool such as OpenDNS, Forcepoint, or Palo Alto that blocks traffic from known malicious websites.



A STRONG BUSINESS **CONTINUITY PLAN**

Ransomware attacks are not random but rather targeted and intentional. Even with the best defenses in place, successful attacks may still occur. Having a strong business continuity plan for recovery could make it easier to avoid paying ransom. **Key components for a business continuity plan to be effective against ransomware include:**

Alignment of recovery objectives to the critical tasks within an acceptable timeframe.

A regular review, update and test of the recovery plan.

Workstations and file servers should not be constantly connected to their back up devices (so that in the event of a successful attack, back ups will not be encrypted). In addition, confirm that your backup solution stores periodic snapshots instead of regular overwrites of previous backups.

Accenture recommends that all organizations review their current processes against these leading practices and close any gaps. And while these recommendations can reduce an organization's vulnerability to ransomware attacks, they may not be fully sufficient as the threat evolves. So we also urge organizations to stay informed about emerging threats and the latest practices required to avoid those threats.

APPENDIX
WANACRYPTOR IOCS AND DETECTION SIGNATURES

iDefense recommends blocking network traffic involving the following URLs and domains:

gx7ekbenv2riucmf.onion
57g7spgrzlojinas.onion
xxlvbrloxvriy2c5.onion
76jdd2ir2embyv47.onion
cwwnhwhlz52maqm7.onion
hxxp://193.23.244.244:443
hxxp://217.79.179.177:9001
hxxp://178.16.208.58:443
hxxp://86.59.21.38:443
hxxp://91.121.83.108:41962
hxxp://104.131.11.214:8080
czrrumvbl5ck6s3ma.net
bnq7nevohqmz45d43n.com
b4e6t3df.net
rddetpruqlmh2.com
gljc5nmgzacv.net
gjgwfrwmefhyrr2evy.com
76ylh2uax.net
w64mek2oznzvkf.com

Detection signatures

The following detection signatures can be used to detect an infection:

```
rule EQN_SMB1_PatientZero{
    meta:
        description = "Detection of network traffic towards the 1st
sinkholed domain - kill switch"
        author = "Kiran Bandla - iDefense"
    strings:
       $smb1_free_hole = { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff
fe 00 00 40 00 0c ff 00 00 00 04 11 0a 00 }
        $ipc = "\\\\%s\\IPC$"
        $userid = "__USERID__PLACEHOLDER__"
        $treeid = "__TREEID__PLACEHOLDER__"
        $old_c2 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
    condition:
        $smb1_free_hole and $ipc and $userid and $treeid and $old_c2
}
rule WanaCrypt0r
{
        meta:
            description = "Detects artifacts from WanaCrypt0r Ransomware"
            author = "Leo Fernandes - iDefense"
         strings:
            $a = "WanaDecryptor"
            $b = "Wana Decrypt0r"
            $c = "WanaCrypt0r"
            $d = ".wnry"
            $e = ".WNRY"
            $f = "bitcoin"
            $g = "vssadmin"
            $h = "torproject"
        condition:
            4 of them
}
```

Additionally, iDefense recommends deploying the Emerging Threats Snort rules (https://rules.emergingthreats.net/) identified by SIDs to detect possible exploitations of MS17-010:

2024207	2024213	2024219
2024208	2024217	2024220
2024212	2024218	

Please track the WanaCrypt0r Intelligence Alert in the iDefense IntelGraph for ongoing updates: "Technical Analysis of WanaCrypt0r," https://intelgraph.verisign.com/#/node/intelligence_alert/view/15bae2ae-8743-4526-ae5e-2e595d572302?source=search.

Please find the following related information in the IntelGraph:

Malware family

"WanaCrypt0r," https://intelgraph.verisign.com/#/node/malware_family/view/e891c945-e821-4158-9d62-c20743e0e292?source=search

Detection signatures

"WanaCrypt0r.yara," https://intelgraph.verisign.com/#/node/detection_signature/view/193089a5-bb97-4a3d-a32f-ccabccf98287?source=search

"WanaCrypt0r_SMB.yara," https://intelgraph.verisign.com/#/node/detection_signature/view/aeb5f1bc-555d-423f-99c1-bcb582803840?source=search

Threat group

"SpamTech," https://intelgraph.verisign.com/#/node/threat_group/view/7802308f-0d3c-499c-989b-e60f416ceb27?source=search

Files

"e333604e0d214d03328a854df130377f," https://intelgraph.verisign.com/#/node/file/view/71cfa24e-fa8a-4d96-b558-8e53bb15db7f?source=search

"db349b97c37d22f5ea1d1841e3c89eb4," https://intelgraph.verisign.com/#/node/file/view/13dfa64b-027b-4e37-9ea8-f13b261eac91?source=search

Find out more about the evolving cyber security landscape and what you can do to strengthen your defenses.

CONTACT

Matt Devost
Managing Director, Accenture Security
Cyber Defense
matt.devost@accenture.com

Justin Harvey
Managing Director, Accenture Security
Incident Response & Threat Hunting
justin.harvey@accenture.com

Tom Parker
Managing Director, Accenture Security
Group Technology Office
tom.parker@accenture.com

Josh Ray
Managing Director, Accenture Security
Cyber Threat Intelligence
joshua.a.ray@accenture.com

Visit us at http://www.accenture.com/security

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.