
Cyberbezpieczeństwo
Perspelutywa
zarzadu
2021.10.27
Krzysztof Dyki

CYBERBEZPIECZEŃSTWO

ISO/IEC TS 27100:2020(E)

Cyberbezpieczeństwo to zarządzanie zagrożeniami bezpieczeństwa informacji przetwarzanych w formie cyfrowej na komputerach, w pamięci masowej oraz sieciach.

Do zarządzania cyberzagrożeniami można stosować różne środki kontroli, metody i techniki bezpieczeństwa informacji.

$162 MLD

WARTOŚĆ RYNKU CYBERBEZPIECZEŃSTWA
W ROKU 2020

$418 MLD

PROGNOZOWANA WARTOŚĆ W ROKU 2028

Źródło: Globe Newswire


TOP 15 CYBER THREATS
enisa
1
Malware
2
Web-based attacks
3
Phishing
4
Web application attacks
5
Spam
6
DDoS
7
Identify theft
8
Data breach
9
Insider threat
10
Botnets
11
Physical manipulation, damage, theft and loss
12
Information leakage
13
Ransomware
14
Cyberespionage
15

$8.6 MLN

PRZECIĘTNA STRATA PRZEDSIĘBIORSTWA WYNIKAJĄCA Z CYBERATAKU W 2020 ROKU (USA)

Źródło: Statista


Microsoft
SOLARWINDS
SUNBURST
FIREEYE, US GOVT.
HACKED
WHAT YOU NEED TO KNOW


COLONIAL
PIPELINE

$1 BILION

GLOBALNY KOSZT CYBERATAKÓW W ROKU 2020

Źródło: The Washington Post

ANNUAL THREAT REPORT

Quick Heal
Security Simplified

Top 10 Windows Malware

01 **W32.Pioneer.CZ1**
Threat Level: Medium
Category: File Infector
Method of Propagation: Removable or network drives

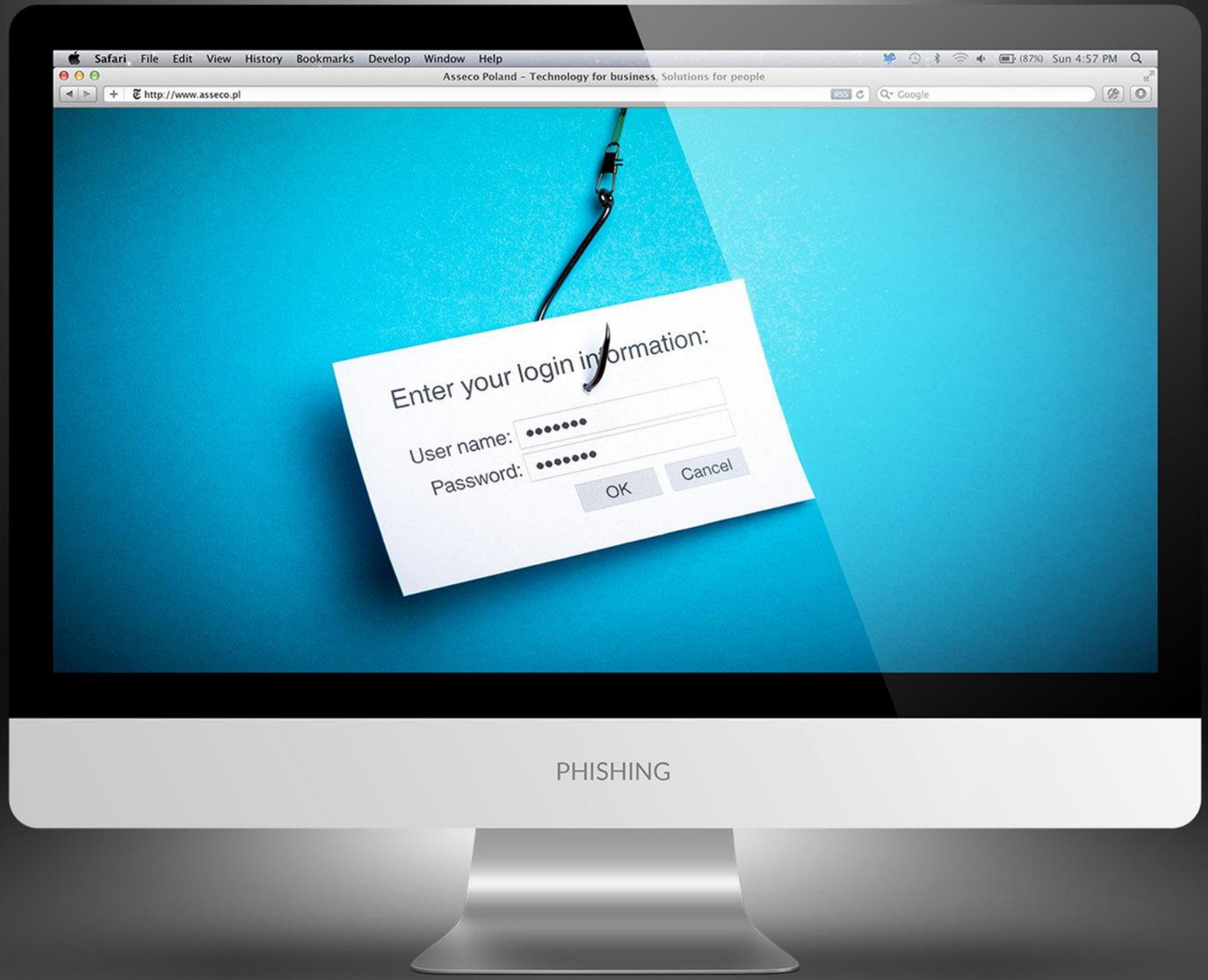
Behaviour:
W32.Pioneer.CZ1 injects its code into files and maliciously collects system information sending it to attackers.

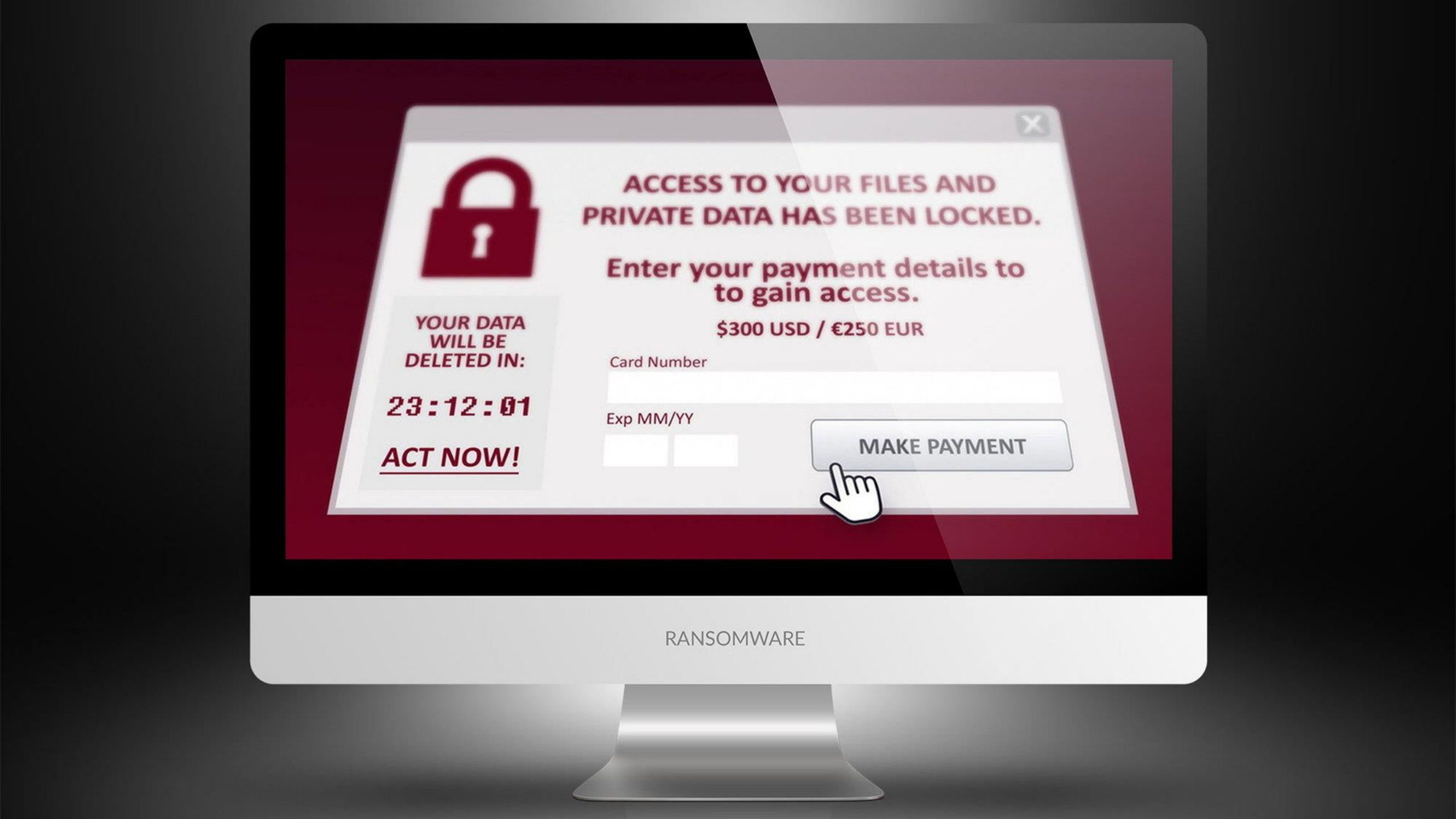
02 **LNK.Cmd.Exploit**
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:
LNK.Cmd.Exploit uses cmd.exe with "/c" command-line option to execute other malicious files simultaneously executing a malicious vbs file which uses Stratum mining protocol for Monero mining.

Trojan.Starter.YY4
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:
Trojan.Starter.YY4 creates a process to run the
alter registry settings which may
like keyloggers, slow
computer


Safari File Edit View History Bookmarks Develop Window Help
Asseco Poland – Technology for business, Solutions for people
http://www.asseco.pl
Google
Enter your login information:
User name:
Password:
OK
Cancel
PHISHING


ACCESS TO YOUR FILES AND
PRIVATE DATA HAS BEEN LOCKED.
Enter your payment details to
to gain access.
$300 USD / €250 EUR
YOUR DATA
WILL BE
DELETED IN:
23:12:01
ACT NOW!
Card Number
Exp MM/YY
MAKE PAYMENT
RANSOMWARE

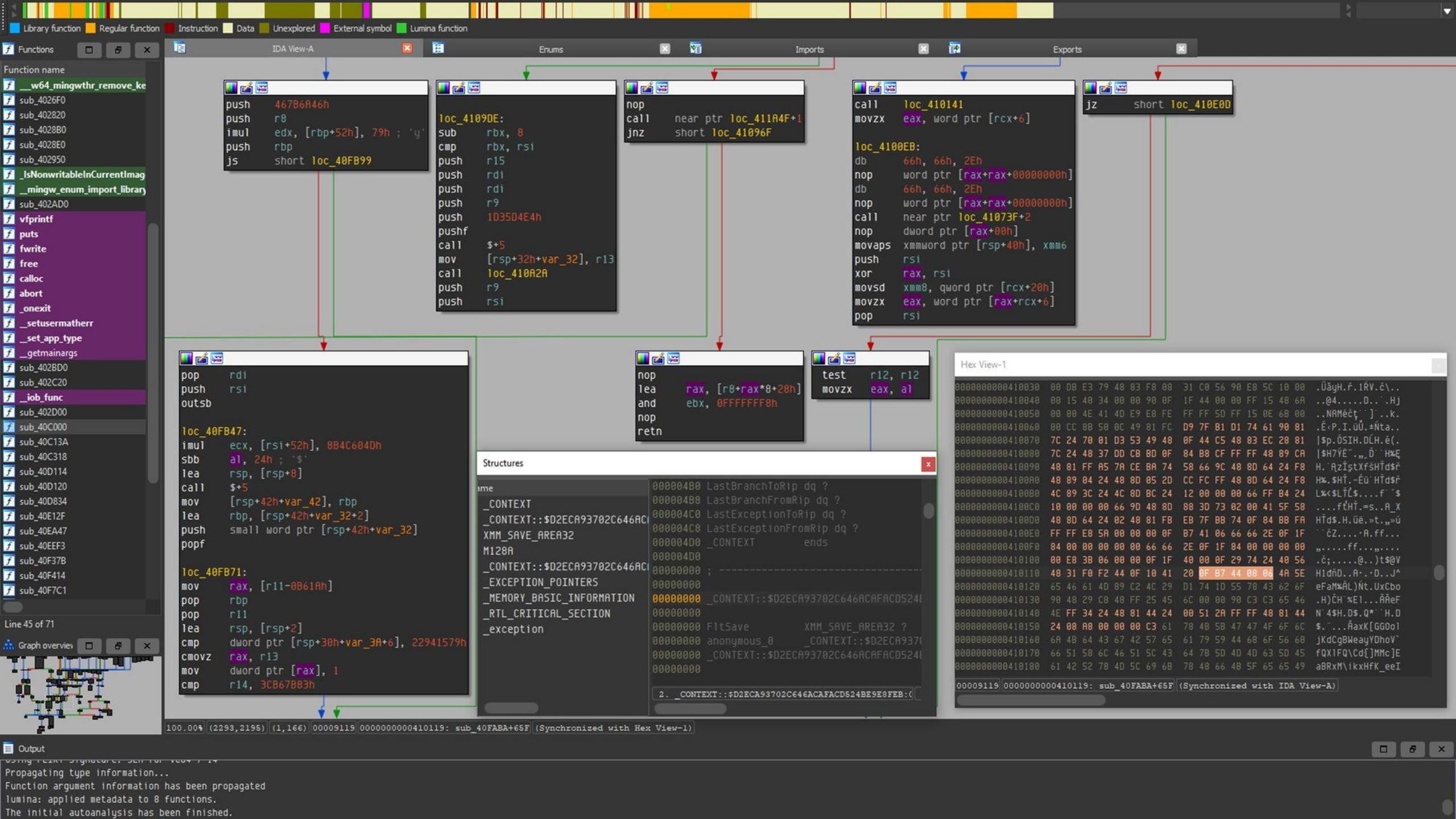
$10 MLN

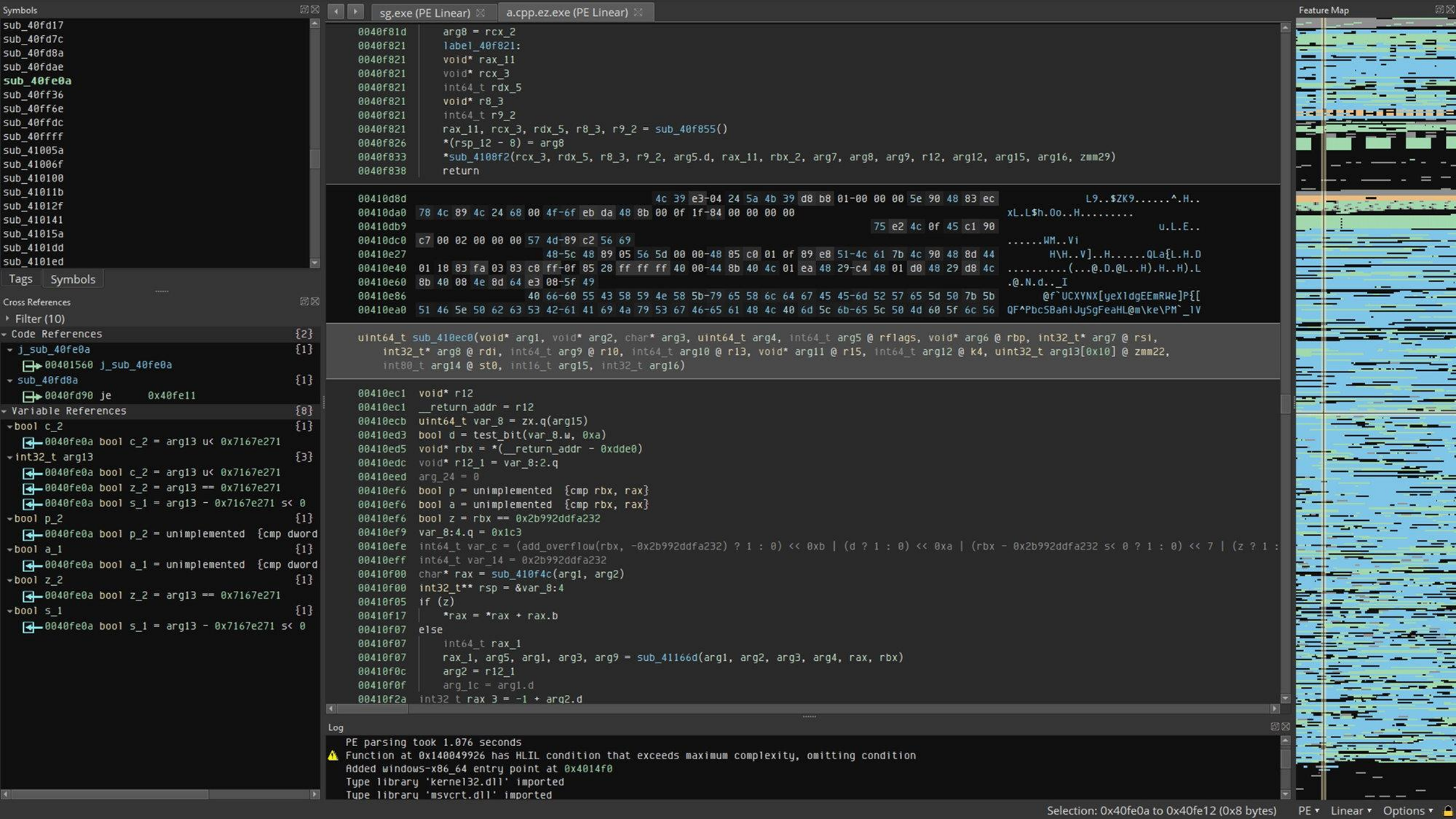
NAJWYŻSZY ZAPŁACONY OKUP
RANSOMWARE W 2020 ROKU

$50 MLN

WARTOŚĆ OKUPU RANSOMWARE
ŻĄDANA W 2021 ROKU

Źródło: ZDNET


Library function
Regular function
Instruction
Data
Unexplored
External symbol
Lumina function
Functions
Function name
__w64_mingwthr_remove_ke
sub_4026F0
sub_402820
sub_4028B0
sub_4028E0
sub_402950
_IsNonwritableInCurrentImag
__mingw_enum_import_library
sub_402AD0
vfprintf
puts
fwrite
free
calloc
abort
_onexit
__setusermatherr
__set_app_type
__getmainargs
sub_402BD0
sub_402C20
__iob_func
sub_402D00
sub_40C000
sub_40C13A
sub_40C318
sub_40D114
sub_40D120
sub_40D834
sub_40E12F
sub_40EA47
sub_40EEF3
sub_40F37B
sub_40F414
sub_40F7C1
Line 45 of 71
Graph overview
IDA View-A
Enums
Imports
Exports
push 467B6A46h
push r8
imul edx, [rbp+52h], 79h ; 'y'
push rbp
js short loc_40FB99
loc_4109DE:
sub rbx, 8
cmp rbx, rsi
push r15
push rdi
push rdi
push r9
push 1D35D4E4h
pushf
call $+5
mov [rsp+32h+var_32], r13
call loc_410A2A
push r9
push rsi
nop
call near ptr loc_411A4F+1
jnz short loc_41096F
call loc_410141
movzx eax, word ptr [rcx+6]
loc_4100EB:
db 66h, 66h, 2Eh
nop word ptr [rax+rax+00000000h]
db 66h, 66h, 2Eh
nop word ptr [rax+rax+00000000h]
call near ptr loc_41073F+2
nop dword ptr [rax+00h]
movaps xmmword ptr [rsp+40h], xmm6
push rsi
xor rax, rsi
movsd xmm8, qword ptr [rcx+20h]
movzx eax, word ptr [rax+rcx+6]
pop rsi
jz short loc_410E0D
pop rdi
push rsi
outsb
loc_40FB47:
imul ecx, [rsi+52h], 8B4C604Dh
sbb al, 24h ; '$'
lea rsp, [rsp+8]
call $+5
mov [rsp+42h+var_42], rbp
lea rbp, [rsp+42h+var_32+2]
push small word ptr [rsp+42h+var_32]
popf
loc_40FB71:
mov rax, [r11-0B61Ah]
pop rbp
pop r11
lea rsp, [rsp+2]
cmp dword ptr [rsp+30h+var_3A+6], 22941579h
cmovz rax, r13
mov dword ptr [rax], 1
cmp r14, 3CB67B83h
nop
lea rax, [r8+rax*8+28h]
and ebx, 0FFFFFFF8h
nop
retn
test r12, r12
movzx eax, al
Structures
_CONTEXT
_CONTEXT::$D2ECA93702C646AC
XMM_SAVE_AREA32
M128A
_CONTEXT::$D2ECA93702C646AC
_EXCEPTION_POINTERS
_MEMORY_BASIC_INFORMATION
_RTL_CRITICAL_SECTION
_exception
000004B0 LastBranchToRip dq ?
000004B8 LastBranchFromRip dq ?
000004C0 LastExceptionToRip dq ?
000004C8 LastExceptionFromRip dq ?
000004D0 _CONTEXT ends
00000000 FltSave XMM_SAVE_AREA32 ?
00000000 anonymous_0 _CONTEXT::$D2ECA937
Hex View-1
100.00% (2293,2195) (1,166) 00009119 0000000000410119: sub_40FABA+65F (Synchronized with Hex View-1)
Output
Propagating type information...
Function argument information has been propagated
lumina: applied metadata to 8 functions.
The initial autoanalysis has been finished.


Symbols
sub_40fd17
sub_40fd7c
sub_40fd8a
sub_40fdae
sub_40fe0a
sub_40ff36
sub_40ff6e
sub_40ffdc
sub_40ffff
sub_41005a
sub_41006f
sub_410100
sub_41011b
sub_41012f
sub_410141
sub_41015a
sub_4101dd
sub_4101ed
Tags
Symbols
Cross References
Filter (10)
Code References {2}
j_sub_40fe0a {1}
00401560 j_sub_40fe0a
sub_40fd8a {1}
0040fd90 je 0x40fe11
Variable References {8}
bool c_2 {1}
0040fe0a bool c_2 = arg13 u< 0x7167e271
int32_t arg13 {3}
0040fe0a bool c_2 = arg13 u< 0x7167e271
0040fe0a bool z_2 = arg13 == 0x7167e271
0040fe0a bool s_1 = arg13 - 0x7167e271 s< 0
bool p_2 {1}
0040fe0a bool p_2 = unimplemented {cmp dword
bool a_1 {1}
0040fe0a bool a_1 = unimplemented {cmp dword
bool z_2 {1}
0040fe0a bool z_2 = arg13 == 0x7167e271
bool s_1 {1}
0040fe0a bool s_1 = arg13 - 0x7167e271 s< 0
sg.exe (PE Linear)
a.cpp.ez.exe (PE Linear)
0040f81d arg8 = rcx_2
0040f821 label_40f821:
0040f821 void* rax_11
0040f821 void* rcx_3
0040f821 int64_t rdx_5
0040f821 void* r8_3
0040f821 int64_t r9_2
0040f821 rax_11, rcx_3, rdx_5, r8_3, r9_2 = sub_40f855()
0040f826 *(rsp_12 - 8) = arg8
0040f833 *sub_4108f2(rcx_3, rdx_5, r8_3, r9_2, arg5.d, rax_11, rbx_2, arg7, arg8, arg9, r12, arg12, arg15, arg16, zmm29)
0040f838 return
00410d8d 4c 39 e3 04 24 5a 4b 39 d8 b8 01 00 00 00 5e 90 48 83 ec L9..$ZK9.....^.H..
00410da0 78 4c 89 4c 24 68 00 4f 6f eb da 48 8b 00 0f 1f 84 00 00 00 00 xL.L$h.Oo..H.....
00410db9 75 e2 4c 0f 45 c1 90 u.L.E..
00410dc0 c7 00 02 00 00 00 57 4d 89 c2 56 69 .....WM..Vi
00410e27 48 5c 48 89 05 56 5d 00 00 48 85 c0 01 0f 89 e8 51 4c 61 7b 4c 90 48 8d 44 H\H..V]..H.....QLa{L.H.D
00410e40 01 18 83 fa 03 83 c8 ff 0f 85 28 ff ff ff 40 00 44 8b 40 4c 01 ea 48 29 c4 48 01 d0 48 29 d8 4c .....(...@.D.@L..H).H..H).L
00410e60 8b 40 08 4e 8d 64 e3 08 5f 49 .@.N.d._I
00410e86 40 66 60 55 43 58 59 4e 58 5b 79 65 58 6c 64 67 45 45 6d 52 57 65 5d 50 7b 5b @f`UCXYNX[yeXldgEEmRWe]P{[
00410ea0 51 46 5e 50 62 63 53 42 61 41 69 4a 79 53 67 46 65 61 48 4c 40 6d 5c 6b 65 5c 50 4d 60 5f 6c 56 QF^PbcSBaAiJySgFeaHL@m\ke\PM`_lV
uint64_t sub_410ec0(void* arg1, void* arg2, char* arg3, uint64_t arg4, int64_t arg5 @ rflags, void* arg6 @ rbp, int32_t* arg7 @ rsi,
int32_t* arg8 @ rdi, int64_t arg9 @ r10, int64_t arg10 @ r13, void* arg11 @ r15, int64_t arg12 @ k4, uint32_t arg13[0x10] @ zmm22,
int80_t arg14 @ st0, int16_t arg15, int32_t arg16)
00410ec1 void* r12
00410ec1 __return_addr = r12
00410ecb uint64_t var_8 = zx.q(arg15)
00410ed3 bool d = test_bit(var_8.w, 0xa)
00410ed5 void* rbx = *(__return_addr - 0xdde0)
00410edc void* r12_1 = var_8:2.q
00410eed arg_24 = 0
00410ef6 bool p = unimplemented {cmp rbx, rax}
00410ef6 bool a = unimplemented {cmp rbx, rax}
00410ef6 bool z = rbx == 0x2b992ddfa232
00410ef9 var_8:4.q = 0x1c3
00410efe int64_t var_c = (add_overflow(rbx, -0x2b992ddfa232) ? 1 : 0) << 0xb | (d ? 1 : 0) << 0xa | (rbx - 0x2b992ddfa232 s< 0 ? 1 : 0) << 7 | (z ? 1 :
00410eff int64_t var_14 = 0x2b992ddfa232
00410f00 char* rax = sub_410f4c(arg1, arg2)
00410f00 int32_t** rsp = &var_8:4
00410f05 if (z)
00410f17 *rax = *rax + rax.b
00410f07 else
00410f07 int64_t rax_1
00410f07 rax_1, arg5, arg1, arg3, arg9 = sub_41166d(arg1, arg2, arg3, arg4, rax, rbx)
00410f0c arg2 = r12_1
00410f0f arg_1c = arg1.d
00410f2a int32_t rax_3 = -1 + arg2.d
Log
PE parsing took 1.076 seconds
Function at 0x140049926 has HLIL condition that exceeds maximum complexity, omitting condition
Added windows-x86_64 entry point at 0x4014f0
Type library 'kernel32.dll' imported
Type library 'msvcrt.dll' imported
Feature Map
Selection: 0x40fe0a to 0x40fe12 (0x8 bytes)
PE
Linear
Options

NIELIMITOWANY BUDŻET

BANK OF AMERICA NA CYBERBEZPIECZEŃSTWO

Źródło: Forbes

APT
...WEDŁUG ROSJI

ITS
CHMURA
INTERNET RZECZY
TECHNOLOGIE MOBILNE


KONTROLA
KONFIGURACJA

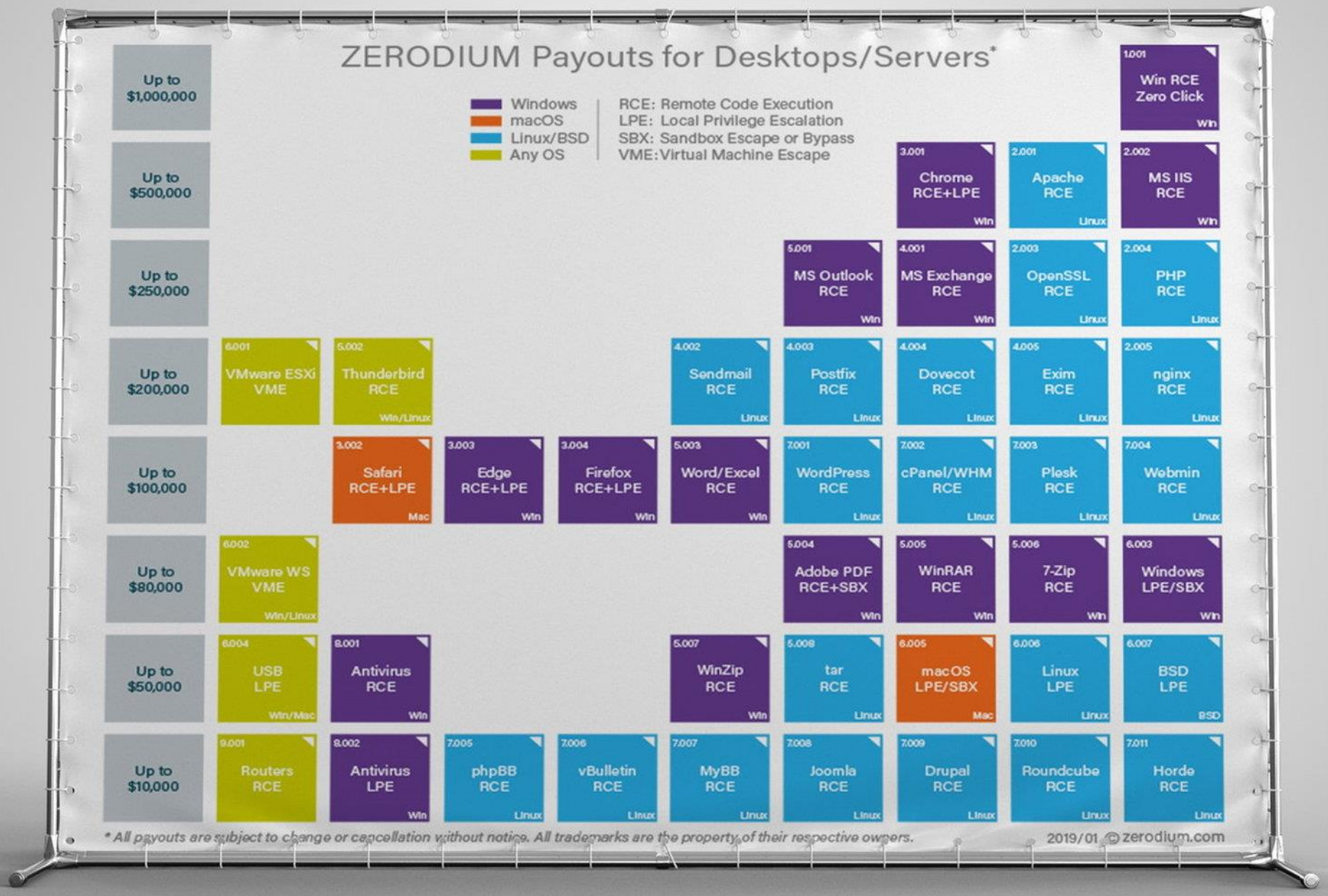
$600 MLN

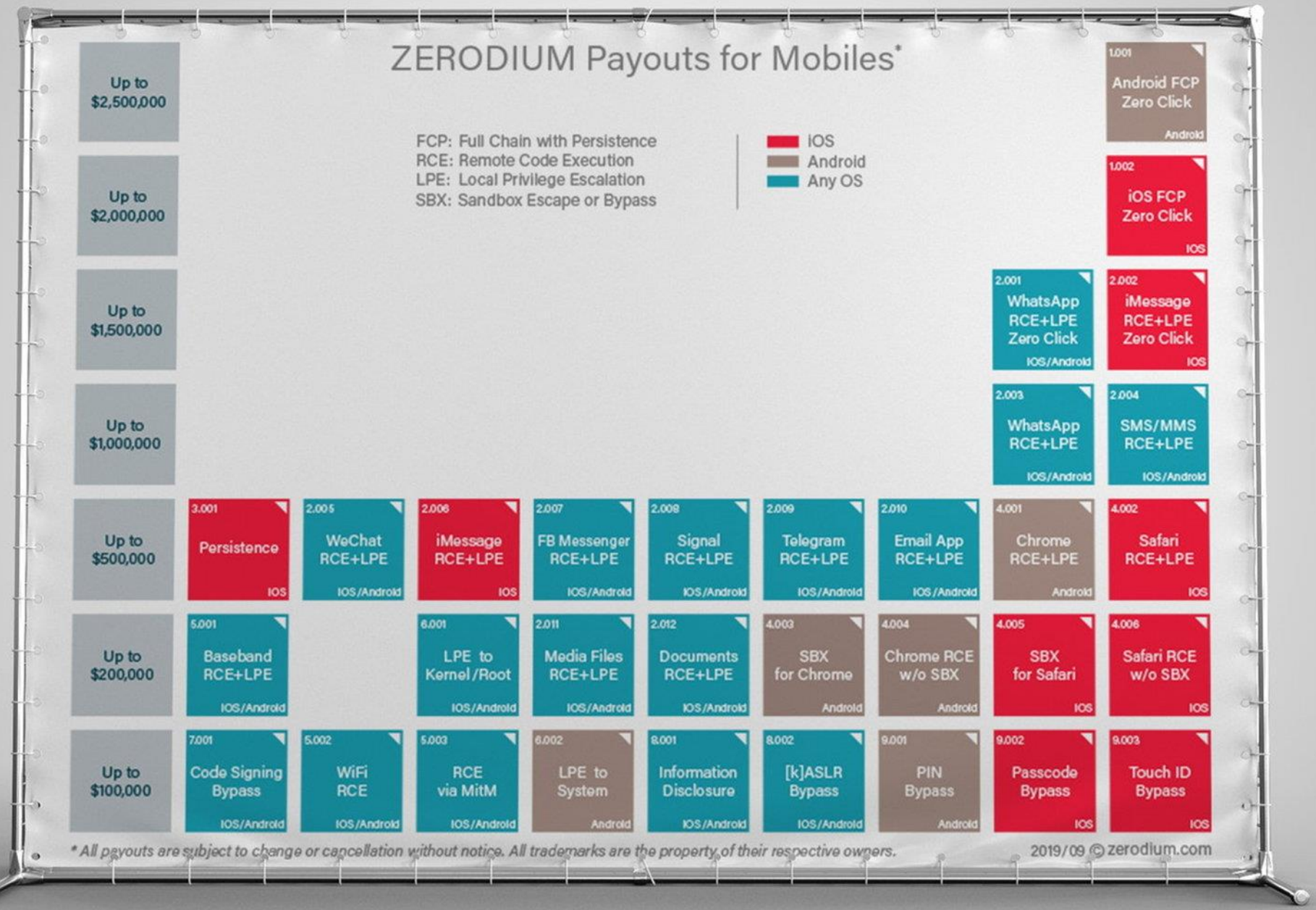
NAJWIĘKSZA KRADZIEŻ WALUTY BTC W WYNIKU JEDNEGO CYBERATAKU

Źródło: Comparitech

CYBERBEZPIECZEŃSTWO A EFEKTYWNOŚĆ OPERACYJNA

RANKINGI


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com


ZERODIUM Payouts for Mobiles*
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $2,500,000
Up to $2,000,000
Up to $1,500,000
Up to $1,000,000
Up to $500,000
Up to $200,000
Up to $100,000
1.001 Android FCP Zero Click Android
1.002 iOS FCP Zero Click iOS
2.001 WhatsApp RCE+LPE Zero Click iOS/Android
2.002 iMessage RCE+LPE Zero Click iOS
2.003 WhatsApp RCE+LPE iOS/Android
2.004 SMS/MMS RCE+LPE iOS/Android
3.001 Persistence iOS
2.005 WeChat RCE+LPE iOS/Android
2.006 iMessage RCE+LPE iOS
2.007 FB Messenger RCE+LPE iOS/Android
2.008 Signal RCE+LPE iOS/Android
2.009 Telegram RCE+LPE iOS/Android
2.010 Email App RCE+LPE iOS/Android
4.001 Chrome RCE+LPE Android
4.002 Safari RCE+LPE iOS
5.001 Baseband RCE+LPE iOS/Android
6.001 LPE to Kernel/Root iOS/Android
2.011 Media Files RCE+LPE iOS/Android
2.012 Documents RCE+LPE iOS/Android
4.003 SBX for Chrome Android
4.004 Chrome RCE w/o SBX Android
4.005 SBX for Safari iOS
4.006 Safari RCE w/o SBX iOS
7.001 Code Signing Bypass iOS/Android
5.002 WiFi RCE iOS/Android
5.003 RCE via MitM iOS/Android
6.002 LPE to System Android
8.001 Information Disclosure iOS/Android
8.002 [k]ASLR Bypass iOS/Android
9.001 PIN Bypass Android
9.002 Passcode Bypass iOS
9.003 Touch ID Bypass iOS
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/09 © zerodium.com

$710 MLN

WARTOŚĆ DOFINANSOWANIA ONETRUST W CIĄGU OSTATNICH 18 MIESIĘCY

Źródło: Cybersecurity Ventures

SOCJOTECHNIKA FUNDAMENT ATAKU

MALWARE - EWOLUCJA TECHNOLOGICZNA

$285 TYS

ŚREDNIE WYNAGRODZENIE DYREKTORA D/S CYBERBEZPIECZEŃSTWA W 2021 ROKU (USA)

Źródło: Salary.com


TESTY BEZPIECZEŃSTWA
CHARAKTERYSTYKA
NIESKUTECZNOŚĆ

3.5 MLN

LICZBA WAKATÓW W GLOBALNYM RYNKU CYBERBEZPIECZEŃSTWA W 2021 ROKU

Źródło: Cybersecurity Ventures

BEZPIECZEŃSTWO HASEŁ, 2FA


ŚWIADOMOŚĆ
FUNDAMENT BEZPIECZEŃSTWA

$7.8 MLD

WARTOŚĆ GLOBALNEGO RYNKU POLIS CYBERBEZPIECZEŃSTWA W ROKU 2020

Źródło: Channel Futures

ROLA ZARZĄDU I NADZORU


Koniec
Dziękuję za uwagę