باسمه تعالی

تحلیل فنی باج افزار PSCrypt

مقدمه :

رصد فضای سایبری در حوزه باج‌افزار، از ظهور نسخه جدید باج افزار PSCrypt خبر می‌دهد. فعالیت این نسخه از باج‌افزار در اواخر ماه آوریل سال ۲۰۱۸ میلادی مشاهده شده است. این باج‌افزار ابتدا در سال ۲۰۱۷ کشف شد و اغلب کاربران خانگی و سازمان‌های اوکراین را مورد هدف قرار داده بود. به نظر می رسد این باج‌افزار از خانواده باج افزارهای GlobeImposter ("GI") باشد. مشاهدات حاکی از آن است که باج افزار پس از نفوذ به سیستم قربانی و اتمام فرایند رمزگذاری فایل‌ها، به انتهای آن‌ها پسوند docs. را اضافه می‌کند و پیغام باج‌خواهی را به صورت یک فایل با نام docs document.html. در هر مکانی که رمزگذاری انجام شده و همچنین بر روی دسکتاپ قربانی قرار می‌دهد. نکته‌ای که در خصوص این باج افزار وجود دارد این است که این باج‌افزار بعد از رمزگذاری و قرار دادن پیغام باج‌خواهی، فایل اجرایی خود را از بین می‌برد.

مشخصات فایل اجرایی :

نام فایل	xls.scr
MD٥	aec٥٤٩٨f٩٥a١٩ac١٤٣٥٣٤٢٨٣٥٩٢٥٤٤b٤
SHA-١	٣٥١d٠٤٣a٠٩٥٥٧١٤٠٣١d١٩٨٩e٠٠d٩fe٣b٨٤eaa٨٢٣
SHA-٢٥٦	٤٣٥٨٤bfbv٩١٠٤٧af٥٩٢c٨٨٣b٨٧٠٧٢٨٩١٣٧٠٨٢f٠٢٤a٨٥١b٠٨٢٧٦٢d٣١٠٠f١f٠٩٤١
اندازه فایل	٣٦٨ KB
کامپایلر	VC٨ -> Microsoft Corporation

فایل اجرایی این باج افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٦٤	٠x١٠٠٠	٠x٢c١٦٥	٠x٢d٠٠٠
.rdata	٥.٩٤	٠x٢e٠٠٠	٠xe٧٧e	٠xf٠٠٠
.data	٣.٥٨	٠x٣d٠٠٠	٠x٦٧١٨	٠x٣٠٠٠
.rsrc	٦.٧٧	٠x٤٤٠٠٠	٠x٢٩٥٨٠	٠x١c٠٠٠

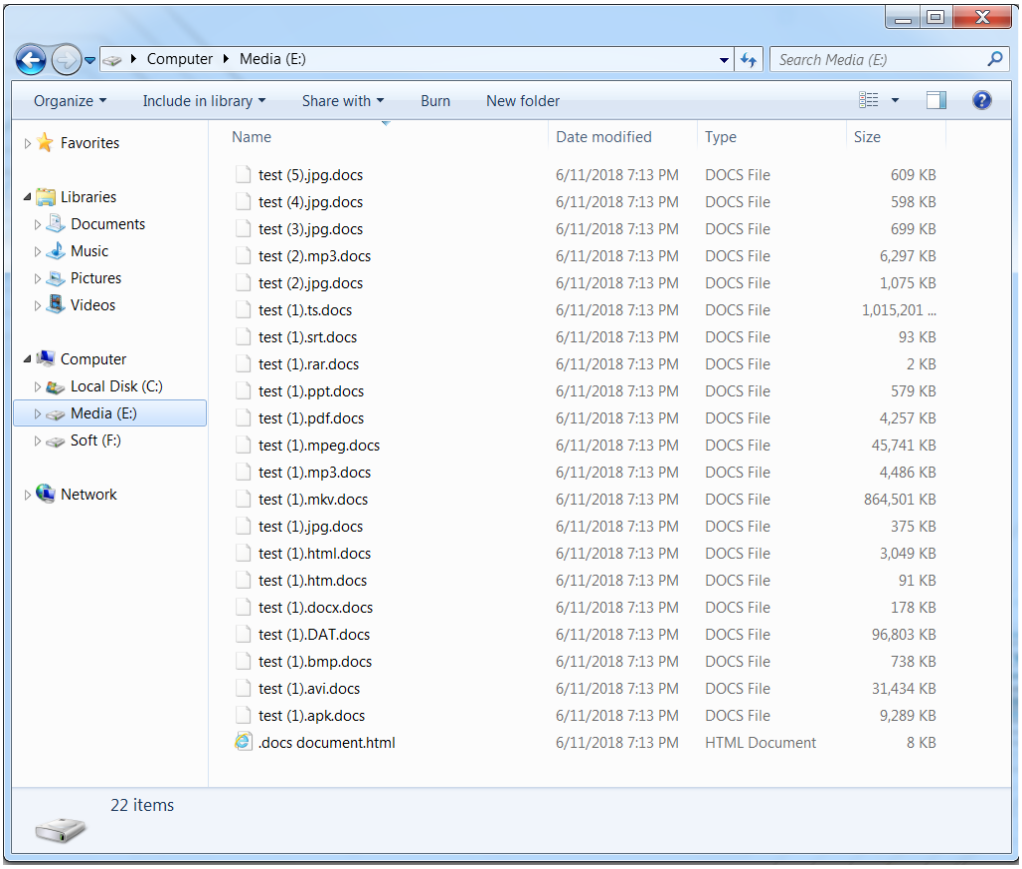
تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار PSCrypt ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. فرآیند اجرای این باج افزار بسیار ساده می باشد ، پس از ورود به سیستم و بررسی محیط آن ، اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می‌کند. این باج‌افزار تمام فایل‌ها به غیر از فایل‌هایی با فرمت زیر را رمزگذاری می‌کند :

```
.$er,.٤db,.٤dd,.٤d,.٤mp,.abs,.abx,.accdb,.accdc
```

آیکن فایل اجرایی این باج‌افزار به صورت زیر می‌باشد :

پس از اتمام رمزنگاری فایل‌های سیستم قربانی به شکل زیر تغییر پیدا می‌کنند :



باج‌افزار PSCrypt در تمام پوشه هایی که فایل های سیستم قربانی را رمزگذاری کرده، یک فایل با نام docs document.html. که در حقیقت همان پیغام باج‌خواهی می باشد، اضافه می‌کند که محتوای آن در تصویر زیر نمایش داده شده است :

ВАШ ЛИЧНЫЙ ИДЕНТИФИКАТОР

19 BF 42 9E 06 A6 D4 C4 86 D0 5B 15 41 02 57 EB 2C 28 20 56 1D 53 14 C5 05 01 07 8A 15 14 86 72 38 55 50 47
4D F1 94 CE 85 CB C9 52 9D D5 A7 3E FE 9C 5C 80 81 00 E7 60 CB A5 34 D1 F5 63 0A C4 A2 27 FF 4A 7F 3C
CC 9F 20 68 5D F2 5B 8D FF 4B 85 32 89 96 27 7A 1C 05 6A 4B 41 D6 AA 36 70 DF 99 32 61 D5 A5 B2 76 86 EC
89 B1 81 A2 2C 7C 0A B5 DE 19 89 49 70 E0 B9 61 52 6C 9C 95 FE 51 1F 2A 1F FD AD 38 9D 90 EC AB F0 B9 30
5B D1 8B 16 6C 89 03 D3 80 8D 14 21 24 4D 86 EA 2A EA C3 F9 D3 D6 E8 00 44 1A 56 66 F1 0D 95 2B 69 2E 32
0F DD 91 28 FC 1E 0F ED 03 4B AD 8C B3 78 F2 7D 41 F6 F0 A8 1B 7B 92 78 A5 D3 2A 74 B4 34 FD 23 D8 84 6E
41 63 5C ED 2B 97 FD 5C 2C 43 74 F4 9C 20 19 3D 14 9D F3 B0 15 0E 25 DA 0F BA D1 07 AB C6 05 3E 41 65 DE
BB A7 D6 28 7C 35 09 B7 7E 3C 1A

☠ ВАШІ ФАЙЛИ ТИМЧАСОВО НЕДОСТУПНІ.☠

ВАШІ ДАНІ БУЛИ ЗАШІВРОВАННИ!

Для відновлення даних потрібно дешифратор.
Щоб отримати дешифратор, ви повинні, оплатити послуги розшифровки:
Оплата відбувається за коштами біткойн на кошелек № 1EoWxYTt7xCskTxjm47E2XNxgkZv1anDP9
Вартість послуги складає **150$**
Оплату можна провести в терміналі IBox. або виберіть один з обмінних сайтів на сторінці - https://www.bestchange.ru/privat24-uah-to-bitcoin.html (приклад обмін Приват24 на BTC) також можете скористатися послугами https://e-btc.com.ua

Додаткова інформація:

Програма можемо дешифрувати один файл як доказ того, що у неї є декодер. Для цього необхідно надіслати зашифрований файл - вагою не більше 2 mb, и ваш уникальный идентификационный код, на пошту: systems32x@gmail.com
Более детальная инструкция по оплате: https://btcu.biz/main/how_to/buy

Увага!

Всі файли розшифровуються тільки після 100% оплати
Ви дійсно отримуєте дешифратор після оплати
Не намагайтеся видалити програму або запустити антивірусні інструменти це може ускладнити вам роботу
Спроби самодешіфрованія файлів приведуть до втрати ваших даних
Декодери інших користувачів не сумісні з вашими даними, оскільки унікальний ключ шифрування кожного користувача.
За запитом користувачів, надаємо контакти клієнтів, які вже користувалися послугами нашого сервісу.

ОБОВ'ЯЗКОВО ЗАПИШІТЬ РЕЗЕРВНІ КОНТАКТИ ДЛЯ ЗВ'ЯЗКУ:

systems32x@gmail.com - основний
systems32x@yahoo.com - резервний
Додаткові контакти:
systems32x@tutanota.com - (якщо відповіді не прийшло після 24-х годин)
help32xme@usa.com - (якщо відповіді не прийшло після 24-х годин)
Additional.mail@mail.com - (якщо відповіді не прийшло після 24-х годин)

З повагою
Unlock files LLC
33530 1st Way South Ste. 102
Federal Way, WA 98003
United States

ENGLISH VERSION

ALL DATA IS ENCRYPTED!

For decoding, write to the addresses:
systems32x@gmail.com - Basic
systems32x@yahoo.com - backup
Additional contacts:
systems32x@tutanota.com - (if the answer did not arrive after 24 hours)
help32xme@usa.com - (if the answer did not arrive after 24 hours)
Additional.mail@mail.com - (if the response did not arrive after 24 hours)

پیغام باج‌خواهی به دو زبان اوکراینی و انگلیسی نمایش داده شده است. در زبان اوکراینی آدرس کیف پول بیت‌کوین ۱EoWxYTtVxCskTxjm٤٧E٢XNxgkZv١anDP٩ به قربانی معرفی شده و ۱۵۰ دلار از قربانی برای رمزگشایی فایل ها درخواست گردیده است. طبق بررسی های انجام شده، تاکنون این کیف پول، هیچ تراکنشی نداشته است.

Summary	
Address	1EoWxYTt7xCskTxjm47E2XNxgkZv1anDP9
Hash 160	9765c6dc67d414ae5596a2ca398318466d600ed8
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

مهاجم برای ارتباط با خود دو راه ارتباطی زیر را در پیغام باج‌خواهی معرفی کرده است :

systems۳۲x@gmail.com

systems۳۲x@yahoo.com

در صورت عدم دریافت پاسخ در ۲٤ ساعت اول، سه راه ارتباطی زیر نیز برای قربانی در نظر گرفته شده است :

systems۳۲x@tutanota.com

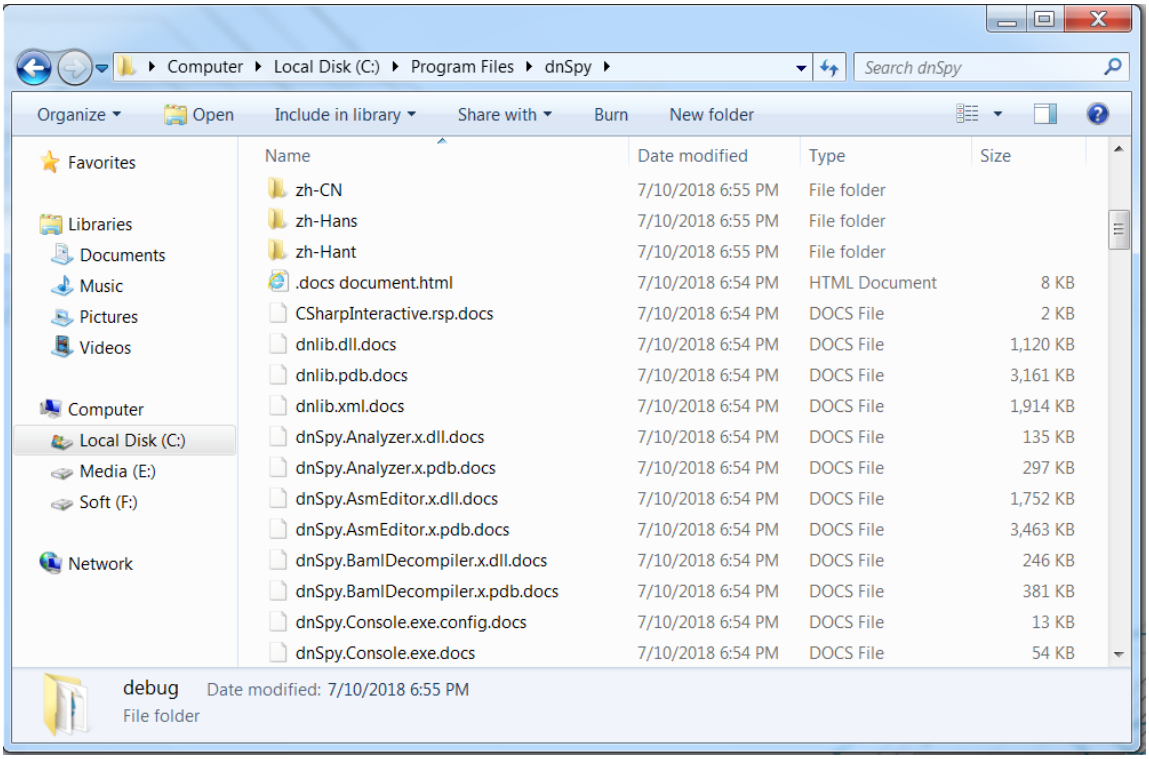
help۳۲xme@usa.com

Additional.mail@mail.com

مهاجم برای جلب اعتماد قربانی از وی درخواست کرده که یک فایل با حجم کمتر از ۲ مگابایـت را بـه همـراه کد ثبت شده در ابتدای پیغام ارسال کند تا آن را رمزگشایی کند .

این باج افزار پس از اتمام فرآیند رمزگذاری، فایل اجرایی خود را از بین برده و دو فایل با نام هـای lab و ico. بر روی دسکتاپ قربانی بر جای می‌گذارد .

نکته جالب توجه اینجاست که باج‌افزار حتی به پوشه Program Files نیز نفوذ کرده و اگر برنامه ای به صورت پرتابل باشد و یا فایلی به صورت دستی اضافه شده باشد و توسط ویندوز نصب نشده باشد نیز، رمزگذاری می‌شود.



تحلیل ایستا:

با بررسی بیشتر کد های باج افزار به نتایج زیر دست یافتیم :

باج افزار پس از حمله به سیستم قربانی، ابتدا مشخصات محیط اجرای خود را بررسی می کند.

```
.text:004020AB          jnz     short loc_4020C4
.text:004020AD          push    offset ProcName ; "GetNativeSystemInfo"
.text:004020B2          push    offset ModuleName ; "kernel32.dll"
.text:004020B7          call    ds:GetModuleHandleA
.text:004020BD          push    eax             ; hModule
.text:004020BE          call    ds:GetProcAddress
```

قطعه کدهای زیر نشان دهنده فایل‌های ایجاد شده lab و ico توسط این باج‌افزار هستند. همانطور که گفتیم این فایل ها پس از اجرای باج‌افزار بر روی دسکتاپ سیستم قربانی ایجاد می گردند.

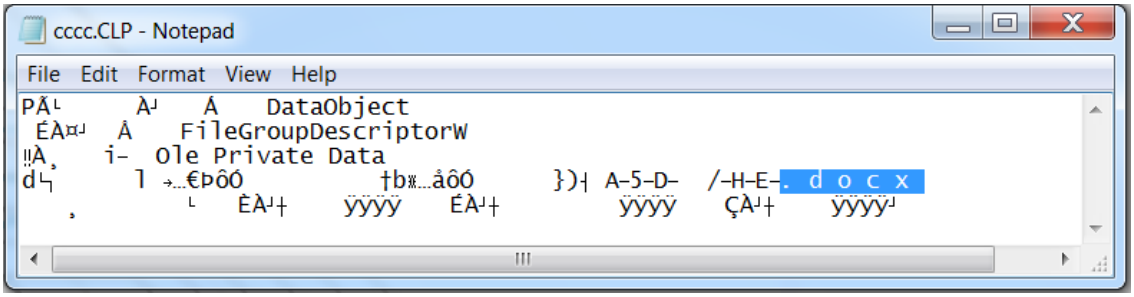
```
.text:004046FB          push    eax             ; pahProfiles
.text:004046FC          mov     [esp+58h+padwIntent], 3
.text:00404707          call    CreateMultiProfileTransform
.text:0040470C          push    offset aRb      ; "rb"
.text:00404711          push    offset a_raw    ; ".raw"
.text:00404716          call    _fopen
.text:0040471B          push    offset aWb      ; "wb"
.text:00404720          push    offset aLab     ; "lab"
.text:00404725          mov     esi, eax
.text:00404727          call    _fopen
.text:0040472C          add     esp, 10h
.text:0040472F          cmp     hdc, 0
.text:00404736          jz      short loc_4047AC
```

```
.text:004048DD          push    0               ; lpSecurityAttributes
.text:004048DF          push    0               ; dwShareMode
.text:004048E1          push    40000000h       ; dwDesiredAccess
.text:004048E6          push    offset a_ico    ; ".ico"
.text:004048EB          call    ds:CreateFileA
.text:004048F1          mov     ecx, [esp+40h+nNumberOfBytesToWrite]
.text:004048F8          push    0               ; lpOverlapped
```

طبق بررسی های صورت گرفته، این باج‌افزار از الگوریتم رمزنگاری RSA استفاده می‌کند.

```
  [0091.286] lstrlenA (lpString="rsa_encrypt") returned 11
  [0091.286] CryptAcquireContextW (in: phProv=0x524cd3c, szContainer=0x0, szProvider=0x0, dwProvType=0x1, dwFlags=0xf0000000 |
ed 1
  [0091.288] CryptGenRandom (in: hProv=0x2f3138, dwLen=0x80, pbBuffer=0x524cd54 | out: pbBuffer=0x524cd54) returned 1
  [0091.288] CryptReleaseContext (hProv=0x2f3138, dwFlags=0x0) returned 1
  [0091.288] lstrlenA
```

بر اساس قطعه کدهای زیر، این باج افزار فایل پیغام باج خواهی خود که با پسوند docx. است را بـا نگهـداری در حافظه کلیپ‌بورد، در هر پوشه که رمزگذاری انجام شده اضافه می‌کند :




```
push    1               ; format
call    ds:IsClipboardFormatAvailable
test    eax, eax
jnz     short loc_403CB9
test    edi, edi
jz      short loc_403CAF
cmp     [esp+40h+var_4], eax
jz      short loc_403CAF
push    eax             ; uType
push    offset Caption  ; "Message"
lea     ecx, [esp+48h+Text]
push    ecx             ; lpText
push    edi             ; hWnd
call    ds:MessageBoxA
```

تغییرات رجیستری :

نتایج حاصل از تحلیل ها نشان می دهد که باج افزار PSCrypt ، کلیدهای رجیستری زیـر را در سیسـتم قربـانی باز می کند :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg۳۲Open Key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

همانطور که ملاحظه می کنید باج افزار، با تغییر مقدار RunOnce به ۱ ، با هر بار ورود کاربر به سیستم، خـودش را اجرا می کند.

```
_alloca_probe () returned 0x40961a
RegOpenKeyExW (in: hKey=0x80000001, lpSubKey="Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce", ulOptions=0x0,
MultiByteToWideChar (in: CodePage=0x0, dwFlags=0x1, lpMultiByteStr=0x4017e8, cbMultiByte=-1, lpWideCharStr=0x0, cchWi
```

تحلیل ترافیک شبکه :

طبق بررسی‌ها و آزمایشات صورت گرفته توسط کارشناسان این مرکز، بر روی باج افـزار PSCrypt، برقـراری ارتباطات شبکه‌ای توسط این باج افزار یافت نشد.

شناسایی :

در حال حاضر تعداد ۵۲ مورد از ۶۸ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Trojan.GenericKD.30648332	AegisLab	Uds.Dangerousobject.Multi!c
AhnLab-V3	Malware/Win32.Generic.C2477193	ALYac	Trojan.Ransom.PSCrypt
Arcabit	Trojan.Generic.D1D3A80C	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/Crypt.ZPACK.decnl
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.30648332	CAT-QuickHeal	Trojan.IGENERIC
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_80% (D)
Cylance	Unsafe	Cyren	W32/Trojan.HMVM-3706
DrWeb	Trojan.Encoder.11539	Emsisoft	Trojan.GenericKD.30648332 (B)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.30648332
ESET-NOD32	Win32/Filecoder.FV	F-Secure	Trojan.GenericKD.30648332
Fortinet	W32/Filecoder.FV!tr	GData	Trojan.GenericKD.30648332
Ikarus	Trojan-Ransom.PSCrypt	Jiangmin	Trojan.Yakes.zny
K7AntiVirus	Trojan (005031101)	K7GW	Trojan (005031101)
Kaspersky	Trojan.Win32.Yakes.wgtk	Malwarebytes	Ransom.FileCryptor
MAX	malware (ai score=96)	McAfee	Ransom-O
McAfee-GW-Edition	BehavesLike.Win32.PUPXAA.fh	Microsoft	Trojan:Win32/Occamy.B
NANO-Antivirus	Trojan.Win32.Yakes.fatdaw	Palo Alto Networks	generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.3fe
Rising	Trojan.Filecoder!8.68 (CLOUD)	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	Ransom.CryptXXX
Tencent	Win32.Trojan.Raas.Auto	TheHacker	Trojan/Filecoder.fv
TrendMicro	TROJ_GEN.R03BC0WDR18	TrendMicro-HouseCall	TROJ_GEN.R03BC0WDR18
VBA32	Trojan.Yakes	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Trojan.Gen	Yandex	Trojan.Yakes!7EzOHaWnYxs
Zillya	Trojan.Yakes.Win32.68464	ZoneAlarm	Trojan.Win32.Yakes.wgtk