Sigurnosne prijetnje na Internetu

Kriminalna skupina Gozi

Kristina Paleka, 6.11.2024

Pregled predavanja

- Kriminalna skupina Gozi
- Zloćudni softver Gozi
- Istaknute varijante
- Obrana i sigurnosne preporuke

Pitanja za ispite

- Koja je primarna funkcija zlođudnog softvera Gozi?
- Kako je Gozi skupina bila strukturirana?
- Koji model usluga je Gozi skupina imala na početku, a koji kasnije?
- Ukratko opišite kako zlođudni softver Gozi krade podatke.
- Nabrojite tri Gozi varijante.

Motivacija

- Zloćudni softver Gozi jedan je od najdugotrajnijih trojanaca za krađu osjetljivih informacija
- Koristi sofisticirane tehnike za infiltraciju sustava
- Stalno se razvija
- Ugrožene strane mogu pretrpjeti značajne financijske gubitke

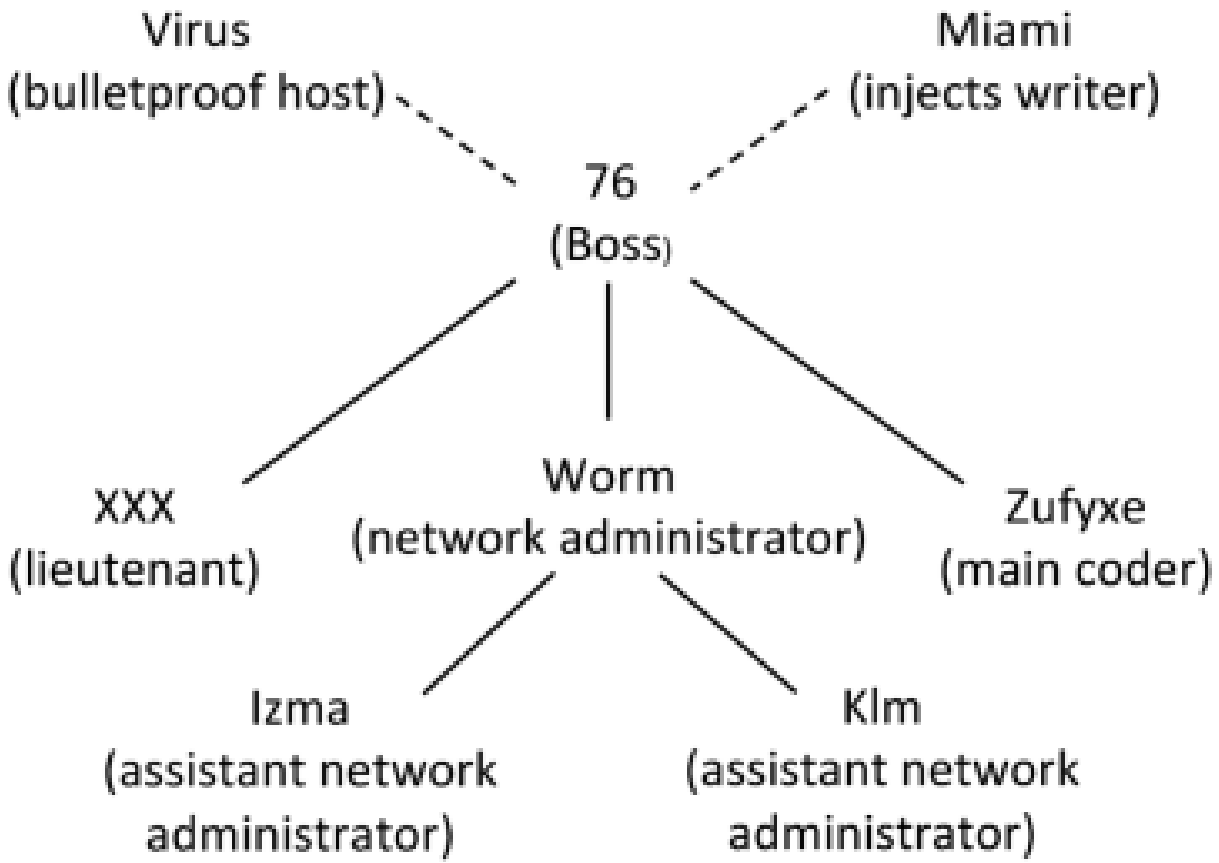
Kriminalna skupina Gozi - Struktura

- **Tvrtka:** “… a firm is a profit-making entity supplying a service or good.” [1]
- **Organizacijske osobine tvrtki:** hijerarhija, definirane uloge i koordinirani napori usmjereni na maksimizaciju profita
- Profiti grupe iznosili su oko 700 000 dolara godišnje

Kriminalna skupina Gozi - Struktura

- **Nikita Kuzmin:** glavni koordinator, organizator i poduzetnik, osiguravao redovite isplate svom timu
- **Specijalizirane uloge:** programeri (“Zufyx”), upravitelji botneta, spameri, novčane mule
- **Slobodni izvođači:** vanjski stručnjaci koji surađuju s više konkurentnih grupa

Struktura Gozi skupine [1]

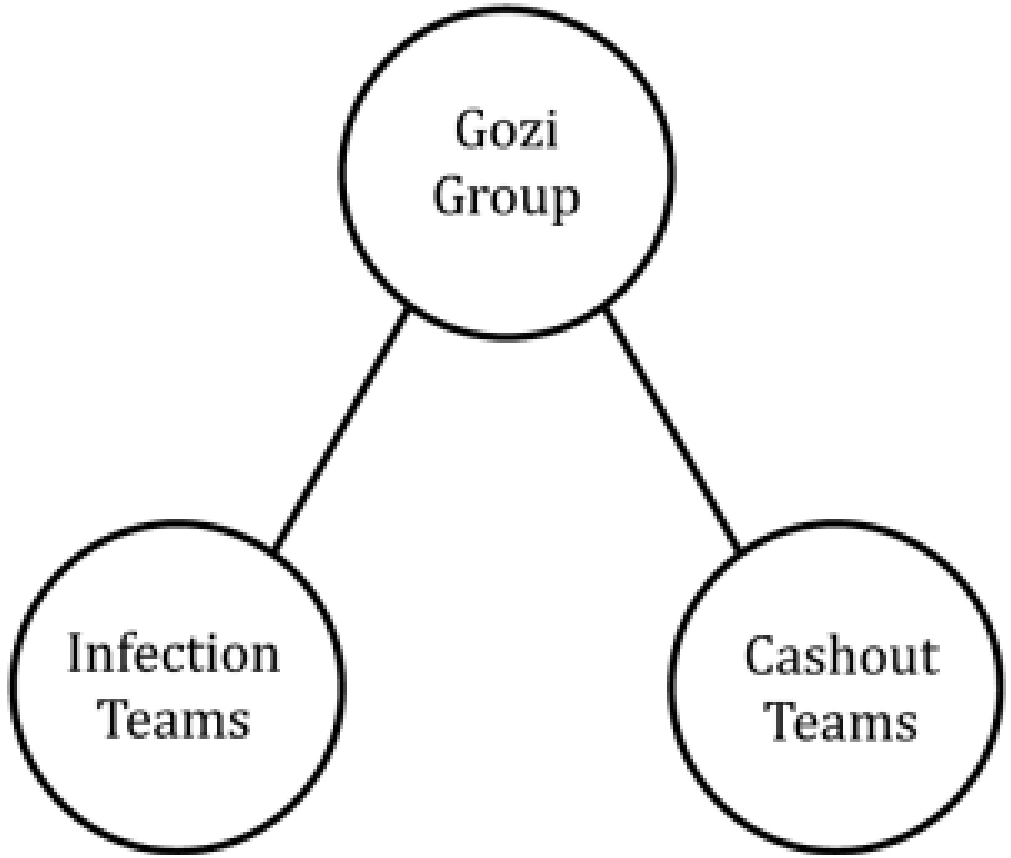


- Bulletproof host odnosi se na usluge poslužitelja koje ignoriraju ili izbjegavaju zahtjeve državnih tijela za provođenje zakona.

Kriminalna skupina Gozi - Model usluga

- U početku **jednokratna prodaja podataka** s kreditnih kartica i prodaja pristupa računima
- Kasnije **partnerski model**: održavanje infrastrukture i iznajmljivanje pristupa botnetu (Malware-as-a-service)
- **Geografski i funkcionalna podjela rada:** povećana operativna fleksibilnost i učinkovitost, izbjegavanje napada na vlastite regije

Partnerski model Gozi skupine [1]



Zloćudni softver Gozi - Otkriće

- Jedan korisnik prijavio je neobičan pristup računu na raznim stranicama
- Analiza njegovog računala je otkrila prethodno neklasificiranu izvršnu datoteku
- Potajno je instaliran 13.12.2006, a detektiran 54 dana nakon, 4.2.2007

Zloćudni softver Gozi - Vektor napada

- **Phishing**: širi se putem e-poruka s poveznicama na kompromitirane web-stranice
- Iskorištavanje ranjivosti zastarjelog preglednika
- Zloćudni softver se preuzima i izvršava na korisnikovom računalu nakon posjeta ugrožene stranice
- Izvršna datoteka (npr. xx_ymvb.exe) pohranjuje se u direktorij korisničkog profila

Zloćudni softver Gozi – Krađa podataka

- **Man-in-the-Browser (MitB) napadi**: ubrizgavanje zlonamjernog koda izravno u proces preglednika žrtve. Ovaj kod mijenja sadržaj web stranica koje korisnik pregledava i hvata podatke prije nego što se šifriraju i pošalju na legitimni poslužitelj

Zlćudni softver Gozi – Krađa podataka

- **Layered Service Provider (LSP):** Gozi se instalira kao slojeviti davatelj usluga (LSP) koristeći *ws2_32.dll* (Winsock2 SPI)
- Winsock2 SPI omogućuje Goziju da "uskoči između" aplikacije (Internet Explorera) i stvarnog mrežnog sloja, presrećući promet prije nego što ga preglednik šifrira pomoću SSL/TLS protokola

Zlćudni softver Gozi – Krađa podataka

- **Ograničenja LSP metode:** funkcionira samo za podatke koje Internet Explorer šalje
- Mnogi sustavi za autentifikaciju koriste AJAX tehnologiju. Ovaj podatkovni promet nije lako uhvatiti LSP metodom, jer AJAX zahtjevi i odgovori funkcioniraju izvan glavnog HTTP zahtjeva

Zloćudni softver Gozi – Krađa podataka

- **Grabs modul:** povezuje se s JavaScript engineom Internet Explorera
- Presreće AJAX zahtjeve i odgovore i zatim ih dodaje u glavni HTTP POST zahtjev koji šalje informacije nazad na C2 (Command and Control) poslužitelj

Primjer rada “grabs” modula [2]

```
URL: https://auth.bigbank.com/siteprotect/image.asp
Data: userID=1045877612&do=signon&passcode=myohmy99


-- grabs ------------------------
URL: https://authserver.bigbank.com/director.asp?GV7tVHGb6
grabs=Individual Accounts
-- grabs ------------------------
URL: https://authserver.bigbank.com/siteprotect/image.asp
grabs=Patricia
-- grabs ------------------------
URL: https://authserver.bigbank.com/siteprotect/image.asp
grabs=Racing
-- grabs ------------------------
URL: https://authserver.bigbank.com/siteprotect/image.asp
grabs=pyramids
```

Zloćudni softver Gozi – Prikrivanjw

- **Upotreba packera:** kompresiraju i prikrivaju kod unutar izvršnih datoteka (WinUpack)
- **Rootkit komponente:** skrivaju prisutnost zloćudnog softvera od standardnih alata za prikaz sustava (Windows Explorer, Windows Registry Editor)

Zloćudni softver Gozi – C2 poslužitelji

- **HTTP POST zahtjevi:** za slanje ukradenih podataka u MIME formatu
- **HTTP GET zahtjevi:** za ažuriranje operativnih parametara (“socks” port)
- Pohrana i organizacija ukradenih podataka
- **Malware-as-a-Service:** klijenti pretražuju i plaćaju specifične podatke, ili iznajmljuju pristup botnet mrežama

Zloćudni softver Gozi – Postojanost

- **Postojanost putem registra i datoteka**: čak i ako se izvršna datoteka ukloni, njeni podaci o konfiguraciji mogu pokrenuti ponovno preuzimanje zloćudnog softvera s C2 poslužitelja
- **Konfiguracija zamjenskih poslužitelja**: Ako primarni C2 poslužitelj padne ili ga uklone vlasti

Zloćudni softver Gozi – Modularni dizajn

- Modularna arhitektura Gozi zloćudnog softvera omogućava ažuriranje **funkcionalnosti** preuzimanjem dodatnih modula s C2 poslužitelja
- **Prilagodba ponašanja**: C2 poslužitelj može prilagoditi ponašanje svake instance zloćudnog softvera (izbjegavaju prikupljanje podataka iz specifičnih geografskih regija)

Zlođudni softver Gozi - Varijante

- **ISFB (Ursnif):** jedna od najranijih i najpoznatijih varijanti Gozi zlođudnog softvera, prilagođena za krađu podataka, posebno putem napada „man-in-the-browser“ (MITB)
- Koristi se za krađu vjerodajnica i osjetljivih informacija kroz napredne injekcije web stranica, obično prilagođene bankarskim stranicama

Zloćudni softver Gozi - Varijante

- **Prinimalka**: prilagođena za velike, automatske financijske prijevare
- Pristup i izvođenje transakcija bez potrebe za ručnim unosom, što omogućuje krađe u širokom opsegu

Zloćudni softver Gozi - Varijante

- **Dreambot**: napredna verzija koja koristi Tor mrežu za prikrivene komunikacije s C2 poslužiteljima
- Promet je teško otkriti
- Koristi dinamičke module za krađu podataka, posebno na financijskim stranicama

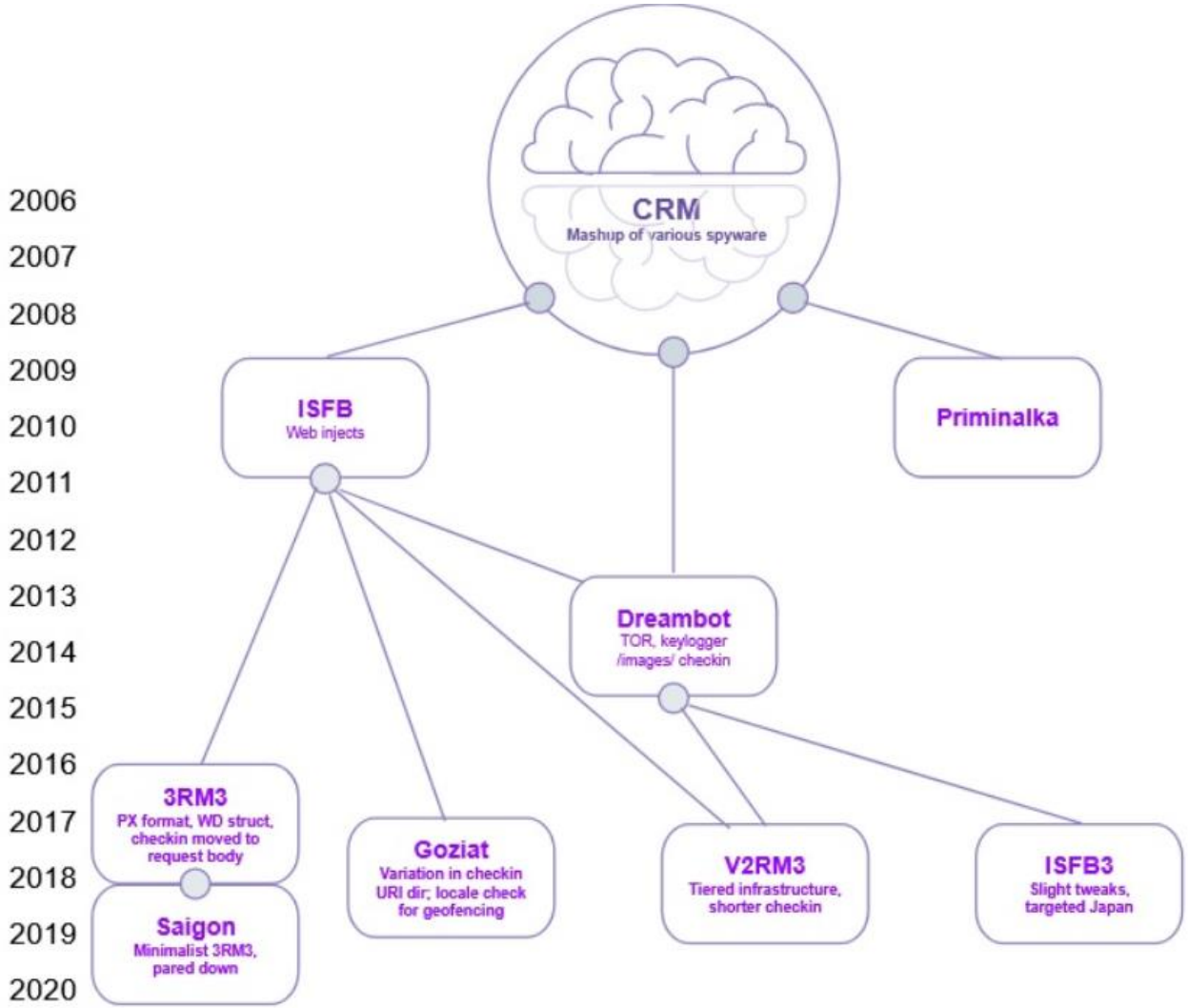
Zloćudni softver Gozi - Varijante

- **GozNym:** Hibrid Gozi i Nymaim zloćudnih softvera koji objedinjuje prilagodljivost Gozija i metode skrivanja Nymaima
- Koristi složenije metode injekcije s boljom mogućnošću prikrivanja svojih tragova
- Često se koristi za napade na velike bankovne sustave, posebno u međunarodnim financijskim transakcijama

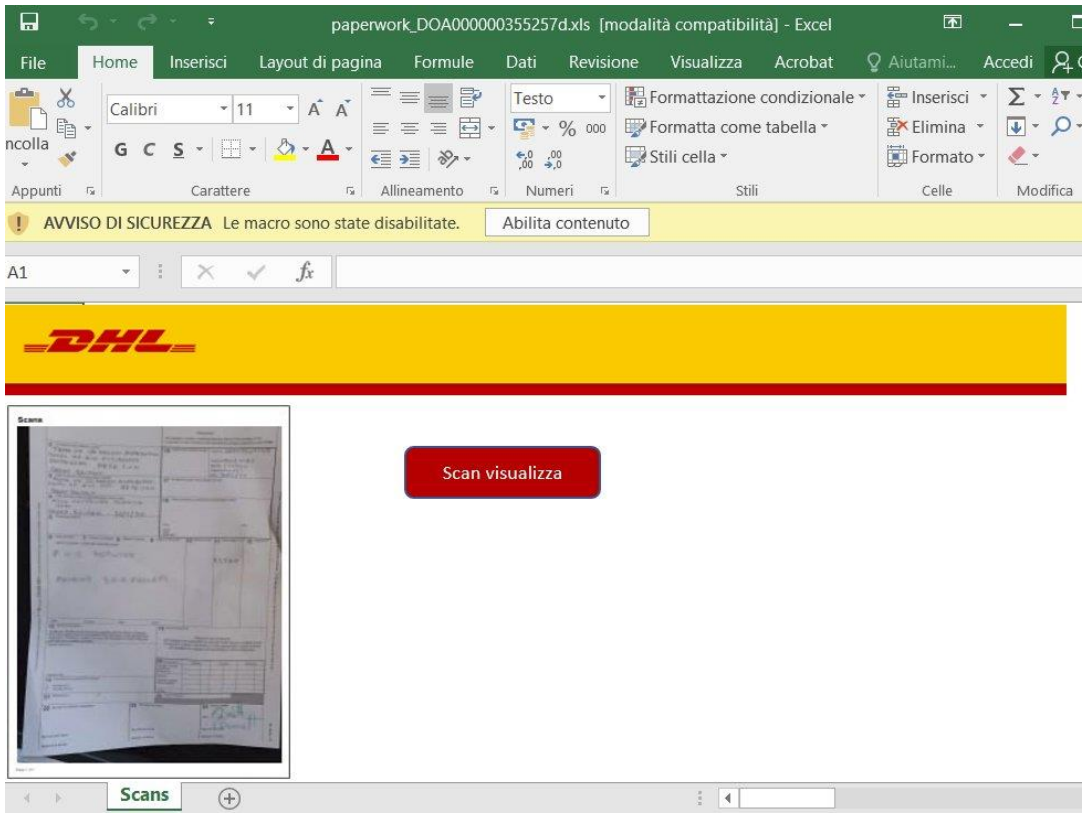
Zlođudni softver Gozi - Varijante

- **Goziat i RM3**: koriste pristup „Living Off the Land“ (LOtL), tj. koriste ugrađene Windows alate za smanjenje vjerojatnosti otkrivanja tradicionalnim alatima
- RM3 koristi prilagođeni PX format za učitavanje DLL-ova (dynamic-link library) i dinamično generiranje ključeva u registrima

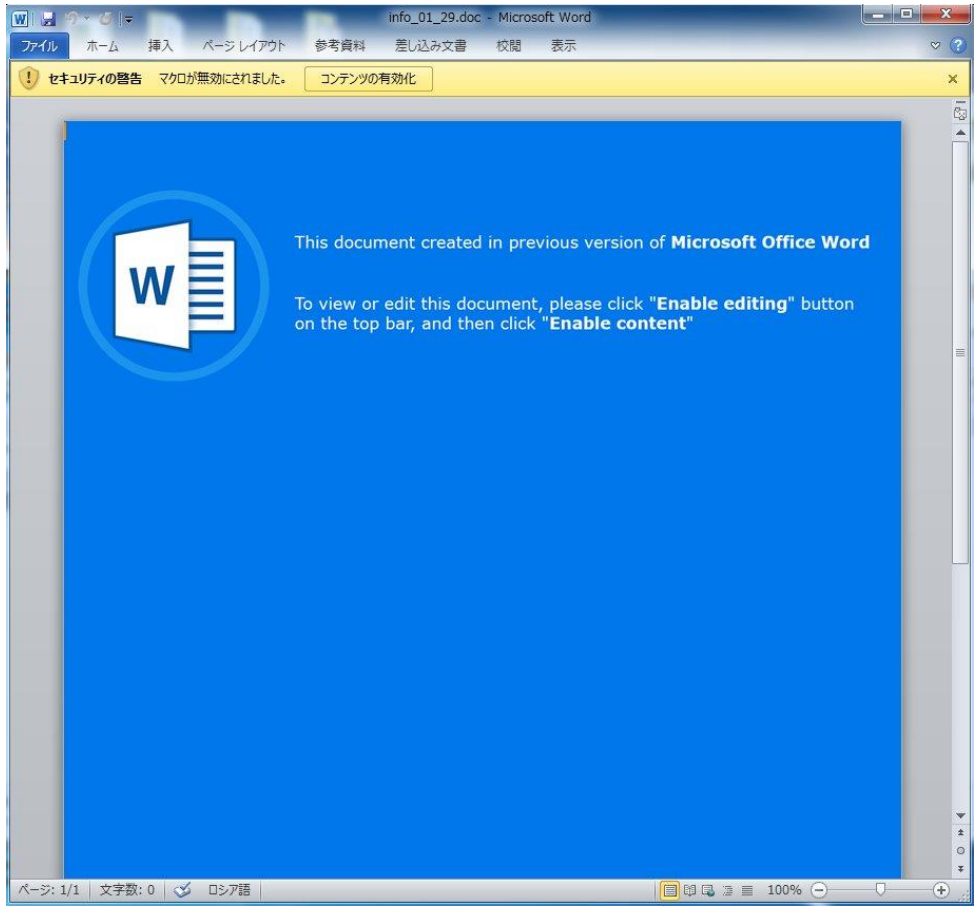
Vremenska linija Gozi varijanti [3]

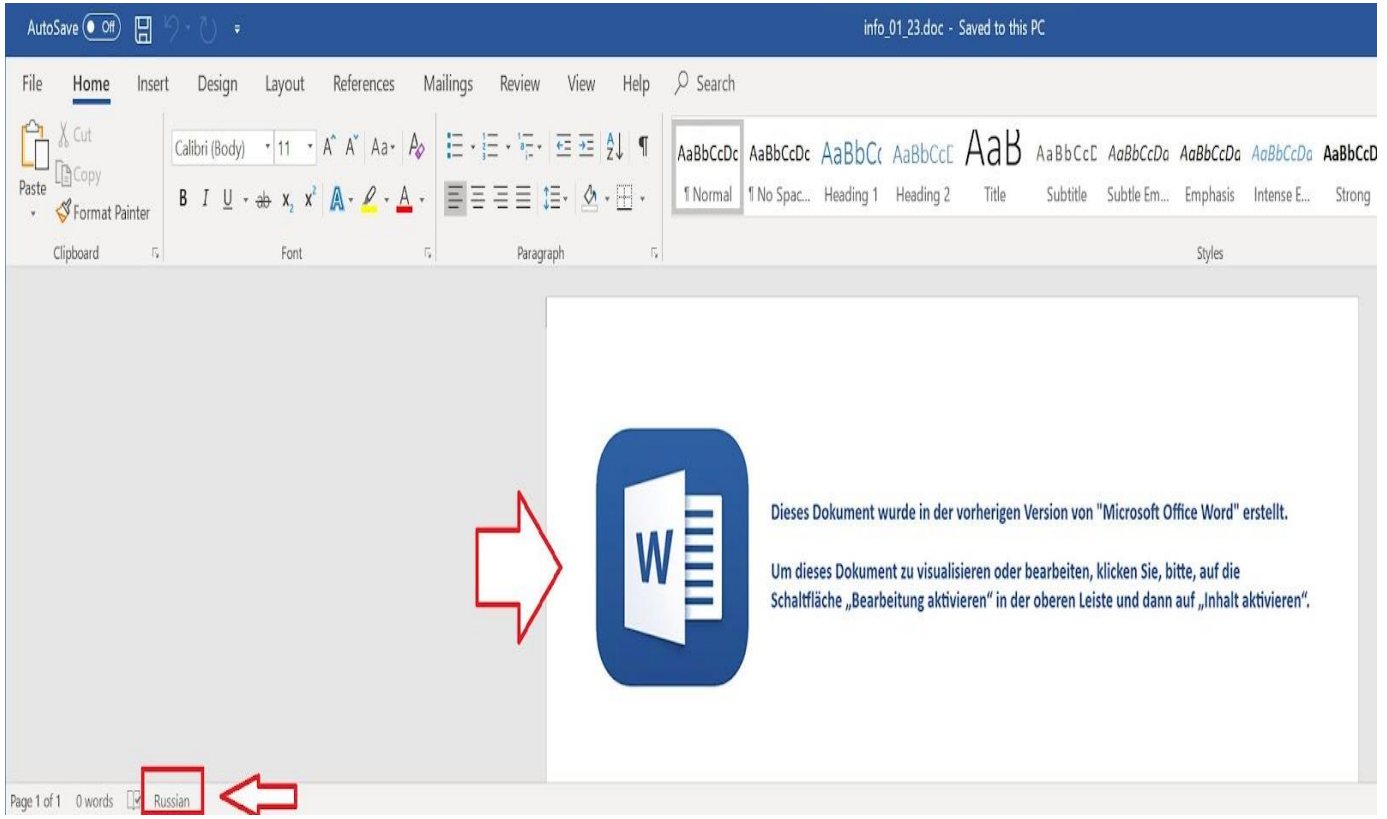


Primjeri dokumenata koji šire Gozi2RM3 [3]



Primjeri dokumenata koji šire Gozi2RM3 [3]





Obrana i sigurnosne preporuke

- **Detekcija ponašanja i mrežna analiza umjesto tradicionalnih potpisa**: tradicionalni potpisi brzo postaju zastarjeli zbog učestalih promjena koda Gozi zlođudnog softvera
- **Anti-rootkit alati i zaštita krajnjih točaka:** Alati koji mogu detektirati rootkit sposobnosti Gozi zlođudnog softvera, kao i neovlaštene izmjene u registrima

Obrana i sigurnosne preporuke

- **Međunarodna suradnja:** Gozijevi poslužitelji često borave u jurisdikcijama s ograničenom suradnjom pa je potrebna je globalna suradnja za učinkovito razbijanje C2 infrastrukture
- **Zaštita korisničkih podataka**: Višefaktorska autentifikacija i šifrirani VPN kanali, redovito ažuriranje softvera

Zaključak

- **Evolucija i prilagodljivost:** razne varijante, modularna arhitektura i metode skrivanja
- **Model Malware-as-a-Service**: rani primjer zlonamjernog softvera u obliku usluge
- **Stalni izazovi za sigurnost:** Prikrivenost i tehnička složenost zahtijevaju napredne metode detekcije

Literatura

- [1] Lusthaus, J., Van Oss, J., & Amann, P. (2023). The Gozi group: **A criminal firm in cyberspace?.** *European Journal of Criminology*, *20*(5), 1701-1718
- [2] Jackson, D. (2007). **Gozi trojan**
- [3] Checkpoint Research, **Gozi: The zločudni softver with a thousand faces**, poveznica: https://research.checkpoint.com/2020/gozi-the-zločudni softver-with-a-thousand-faces/

Dodatna literatura

- Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). **Comprehensive analysis of advanced techniques and vital tools for detecting zlоćudni softver intrusion.** *Electronics*, *12*(20), 4299
- Colajanni, M., Gozzi, D., & Marchetti, M. (2008, September). **Collaborative architecture for zlоćudni softver detection and analysis.** In *IFIP International Information Security Conference* (pp. 79-93). Boston, MA: Springer US

Hvala!