Web Defacement
Root.Dark.Team & Anonymous

Web Defacement The Graffiti Parallels

Joey Hernandez CEH CISSP CISM

Background

- Graffiti
- Roll Call
  - Structure
- Web Defacement
  - Roll Call
  - Attribution

Graffiti

Gang Graffiti is typically used for one of the following purposes:

- Roll call: a list of gang members names (usually nicknames)
- Identification of alliances: lets other gangs know that two or more gangs have formed an alliance
- Declare war: show which gangs are fighting
- Tribute: to pay tribute to a dead member(s) or to warn that someone's marked for death
- Detectives follow the gang graffiti closely to get insight on what's going on in the gang world. They also photograph it for later reference and comparison [1]

Key to the information gleaned from analysis of Gang Graffiti are the external indicators which provide attribution. This information aides predictive analysis

Roll Call Significance

When Graffiti is left on a wall there are key indications about the vandal presented:

- 1 or 2 of the first profiles “nicknames” tagged as part of the roll call are involved with the defacement.
    1. **This is typically the first 2 names of the roll call – the new blood**
- The additional names are “key” organizational players – The Individuals Who Call The Shots
    1. **This is the equivalent to name dropping**
    2. **An effort to impress the “leadership”**
- There is often a claim to a bigger organization
    - A Top Tiered syndication
    - Smaller gangs attempt to affiliate with Latin Kings, Crips, Bloods

Small time organizations try to gain clout by tying themselves to more powerful organizations

Attribution

- The Matrix Of The Message & Roll Call Provides:
  - The vandals significant ties
    - Who includes the individual on their defacement?
  - The vandals methodology in location selection
    - Hidden Locations
      - Back Streets
    - Distant Locations
      - Other Cities, Neighborhoods
    - Significant Locations
      - City Hall, Police Stations, Government Facilities
  - The vandals message
    - Defacement Only
    - Suggestive Message
  - What's left behind?

Web Defacements

The Parallels

Joey Hernandez CEH CISSP CISM

Web Defacement

- hxxp://www.barriovivo.com

- @xllLinuxeroDeatllx
- @Mantr@x
- @AZ4TH0TH
- @Br4nd
- @Pr4X!
- @ThopJuliet(Cloud)
- @Shell|Black
- @Maximus Well
- @_Nitch

- hxxp://www.universinet.it

- @xllLinuxeroDeatllx
- @Mantr@x
- @AZ4TH0TH
- @Br4nd
- @Pr4X!
- @ThopJuliet(Cloud)
- @Shell|Black
- @Maximus Well
- @NodSprut

Notice the common members throughout and with each new instance of defacement an additional

- hxxp://corpoces.edu.co/

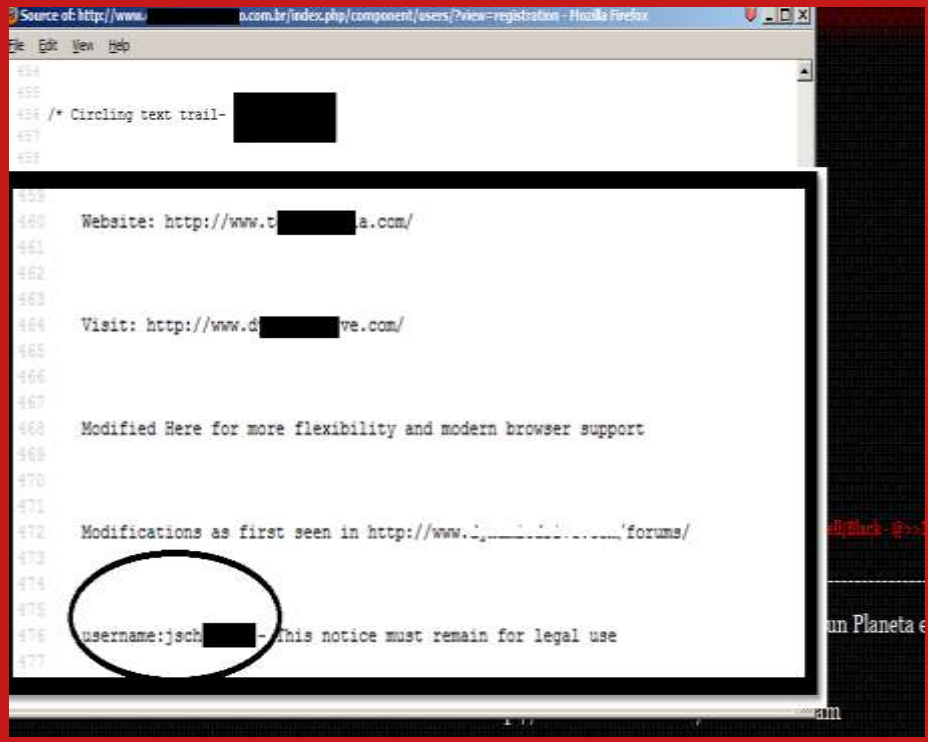
- @xllLinuxeroDeatllx
- @Mantr@x
- @AZ4TH0TH
- @Br4nd
- @Pr4X!
- @ThopJuliet(Cloud)
- @Shell|Black
- @Maximus Well
- @_Nitch
- @H4K3R_RDT

Roll Call Significance

- In these cases @_Nitch, @NodSprut, @H4K3R_RDT were the actual individuals tied to the malicious activity.
- As with graffiti there is an effort to “name drop” the true hackers
- @xllLinuxeroDeatllx - @//Mantr@x// - @<--AZ4TH0TH--> - @\\Br4nd// - @Pr4X!-z - @> - @Shell|Black - @>>Maximus Well<< - @_Nitch
- Additionally, there are efforts to tie the organization to “Anonymous”

Attribution

- The detrimental aspect to “Anonymous”
- Unfocused splinter activity with unskilled participants
  - Joomla or Wordpress Exploits
    - “ The equivalent to tagging in a low lit back alley”
  - Source Code revealed where others could download the script
    - “The equivalent to “Revealing Stash Houses”



Source Code from one of the recent hacks revealed the actual user name

Additional Attribution

- The Pastebin.com hosted code hxxp://pastebin.com/pEHf0E0u is so replicated, the initial script contains additional userid hidden (not so much)
  - Which ties to a flicker account
  - Which ties to a Lastfm account
  - Which ties to a twitter account
  - Which ties to ANONYMOUS followers

Conclusion

- The parallels between modern web defacement and graffiti are tight. The Baby Hackers are going to be one of two things
  - The Demise of The Anonymous Hacktivity
  - Those involved with Root.Dark.Team will be discovered by organizations such as the Zetas, who they've threatened or the Governments who they've been a thorn in the side to.