EMET für den Bridge Rechner einrichten

Man kann EMET auf zwei Arten startenn. Einmal über das normale Startmenü und dann über das Icon im Systray

Emet startet mit folgendem Bildschirm

			Enhanced Mitgation Experier	nce Tookit			- 8	×
i Import Export Group Policy File	Weizerd Appen Trust Configuration	Quick Profile Name: Recommended security setting Maximum security settings Recommended security settings	Windows Event Log Tray Icon Larly Warning Reporting	Help Info ra				
System Status						-		T
Data Exe	cution Prévention (DEP)					1	Application Opt In	
Shuchare	d Exception Handler Overwrite	Protection (SEHCP)					Application Opt In	
Address 1	ipace Layout Randomization (A	G(R)				2	Application Opt In	
Certificat	e Trust (Pinning)					V	Enabled	1
Running Processe	6							
Process ID	Process Name						+ Running EMET	_1.1
1804	conhest - Hest für Konsoleni	crotor						2
3.796	Connectifyd - Connectify Da	ence) Service	das ist dis blats	AAR CARLINS				
1700	ConnectifyService -		uals ist die riots	spor Sonware				
492	caras - Clent-Server-Laufze	(prozess						
432	carss - Client-Server-Laufzei	(prozess						
1888	CyberGhost.Service - Cyber	Chost Service						
	Participa Perintena Manha						C Befresh	£
		Open E Hide	MET	Anpassen				
			¢,0,0	kbps kbps		(0)		
1	· 1 / 1 1	II () O O	1 . *	IDNI CII.	1 1		ידדי 1 ו	/

und man sieht, dass die Hotspot Software und ein VPN Client bereits von EMET überwacht / geschützt werden obwohl zu diesem Zeitpunkt der voreingestellte "recommended" Schutzstatus eingestellt war. Will man den Stutzstatus steigern wählt man oben (an der Curserposition) die "Custtom Security Settings". Um dort hin zu kommen klickt man aus Apps und sieht dann.

				Applic	ation Con	figuration							-		×
Export Export Selected Add Addication Add I	Mildcard Re	emove lected	Show Full Path	Show A Setting	a show	Group Apps	• Stop	e on explai		Deep H	ooks <table-cell></table-cell>	Anti Detoura			
Mitigations				- op aa	-		- Deris	tart mester i			parent and				
Briter test to search -			(2)	Find	Cle	ar i									
App Name	DEP	SEHOP	NIP	Heap	EAF	EAF+	Mand	Botto.,	Load.b	MemP.	Coller	SmEx.	5ladk	ASR	1
OUTLOOKEXE	8	×	2	2	1	0	1	~	8	×.	2	N.	1	1.1	A
WINWORD.EXE	2	8	2	4	2	E	V	2	1	1	~	2	2	V	1
EXCELEXE	1	1	1	1	1		4	~	1	~	2	4	4	4	5
POWERPNT.EXE		4	1	9	1	0	2	9	9	1	9	2	4	¥	5
H5ACCESS.EXE	2	2	2	8	2	10	2	8	8	2	2	2	2		
MSPUBJEXE	1	2	1	4	1	TE	1	4	~	2	4	4	2	TE	£.
INFOPATH.EXE	1	1	4	1	4		4	4	1	1	~	2	4		
VISIO.EXE	2	~	1	8	8	0.0	1	2	9	2	8	8	4		
VPREVIEW.EXE	2	1	~	1	9		2	2	1	2	~	2	×		
LYNCEXE	1	~	8	2	1	D	1	4	4	4	2	4	4	1.6	
PPTVIEW.EXE	1	1		1	2	1.0	~	1	8	1	2	2	~		
OIS.EXE	×	1	2	1	1		~	1	~	×	1	2	4	TO	
AcroRd32.exe	2	~	~	2	1	×	1	1	1	1	1	2	~	TP	
Acrobat.exe	2	9	8	1	4	4	1	1	1	8	4	1	4	T E	
java.exe	1	2	1.12		2		1	8	4	2	2	9	2		
javaw.exe	8	2	1	ET.	R.	0	2	8	8	2	8	8	2	E	
javaws.exe	×	1	2	11	2	1.0	~	2	8	8	2	2	~		v
												OF	16	Class	

Klickt man auf dieser Seite dann auf Add Aplication öffnet sich ein Esplorerfenster mit dem man zu der Exe Datei navigieren kann die man hinzufügen möchte.

Cryptosto			P
rganisieren 👻 Neuer	Ordner		
*	Name	Änderungsdatum	Тур
Bibliotheken	🌙 cpfworkrt	10.04.2017 06:59	Dateiord
Dokumente	🔮 client.exe	10,02,2017 08:22	Anwende
	Csvpn.exed	10.02.2017 08:22	Anwendu
Computer	dnscrypt-proxy.exe	10.02,2017 08:22	Anwendu
Lokaler Datentra	🗾 hostip.exe	10.02.2017 08:22	Anwendu
Benutzer =	obfs4proxy.exe	10.02.2017 08:22	Anwendu
boot	obfsproxy.exe	10.02.2017 08:22	Anwendu
Intel	ssl.exe	10.02.2017 08:22	Anwendu
PerfLogs	rotatelogs.exe	10.02.2017 08:22	Anwendu
portable loois	💽 tap32.exe	10.02.2017 08:22	Anwendi
ProgramData	Tap64.exe	10.02.2017 08:22	Anwendu
🔐 Windows 👻	* m		+
Datei <u>r</u>	ame: client.exe	✓ Executables (*.exe)	•

		cjucionosco y	1.21	ayacı dinar bi bir cispeli			
Organisieren 👻 Neuer	Ordn	er		•			
🔆 Favoriten	Na	me		Änderungsdatum	Тур		
E Desktop		fr		10.04,2017 07:01	Dateio		
📕 Downloads	1	Frameworks		10.04.2017 07:01	Dateio		
		it		10.04.2017 07:01	Dateio		
ᇘ Bibliotheken	14	pl		10.04.2017 07:01	Dateio		
Dokumente	J.	ro		10.04,2017 07:01	Dateic		
		ru		10.04.2017 07:01	Dateio		
🜉 Computer		BsSndRpt.exe		08.03.2017 11:07	Anwer		
🚢 Lokaler Datenträger	100	CyberGhost.exe		08.03.2017 11:07	Anwei		
👝 Lokaler Datenträger		CyberGhost.Set		08,03,2017 11:07	Anwei		
ASUS Tools (E:)		PeLauncher.exe		08.03.2017 11:07	Anwer		
	0	unins000.exe	10.04.2017 07:01 Am				
🗣 Netzwerk	0	wyUpdate.exe		06.09.2012 00:04	Anwer		
	1	m	_		*		
Dateij	name:	CyberGhost.exe	Executables (*,exe)				

und nachdem man sie ausgewählt hat erscheint sie dann unter den automatisch hinzugefügten Programmen.

Puport Spiected Pile Add Application Add V Add Application Add V Add / Ren Mitigations Emer land fla search App Nome MSPUB-EXE DisFORATHEXE VYREVIEW.EXE LVINC.EXE PPTVIEW.EXE	Widcard Re Se nove	SEHOP	Show Full Path	Show A Setting Option	Show Policy Cle	Group Apps	Stop Agdt Defau	on exploit only It Action	2.2	E Deep Ho Banned Mittg	oks 🗹 Punction ation Set	Anti Detouri s tings	•		
Export Selected Add Application Add V File Add Application Add V File Add / Ren Nitigations Emer Lest It a search App Name HSPUBLEXE DIFOPATHLEXE VISIOLIXE VIPROPATHLEXE LYINCLEXE PPTVIEWLEXE	Vildcand Re Se nove DEP	sected sected sector	Show Full Path	Show A Setting Option	Cle	Group Apps) Audit Defau	ionly It Action		Banned Mittg	Function ation Set	s tings			
Selected File Add / Ren Mitigations Enter/ test to search App Nome MSPUBLEXE DIFOPATHLEXE VISIOLIXE VISIOLIXE VIPREVIEW.EXE LYINC.EXE PPTVIEW.EXE	se nové DEP	sected sector	Path	Setting Option Find	Cles	Apps	Defau	Action		Ming	ation Set	tings			
File Add / Ren Mitigations Enter/ test is search App Nome MSPUBLEXE DIFOPATHLEXE VISIOLIXE VIPECEXE LYINCEXE LYINCEXE PPTVIEW.EXE	DEP	SEHOP	14	Optor Find	Cle		Defau	At Action		Mitto	ation Set	tings			
Miligations Enter last la search App Name MSPUBLEXE ENFOPATHLEXE VISIOLEXE VPREVIEW.EXE LYNKLEXE EVPREVIEW.EXE PPTVIEW.EXE	N N N	SEHOP	NulPers	Find	Cle	Sr									
App None MSPUBJEXE BIFOPATHLEXE VISIOLEXE VPREVIEW.EXE LYNKLEXE PPTVIEW.EXE	N N N	SEHOP	14. NulP	Find	Cle	ar I									
App Name MSPUBJEXE DIFOPATHLEXE VISIOLEXE VPREVIEW.EXE LYNCLEXE PPTVIEW.EXE	DEP X X	SEHOP	NJP												
HSPUBLEXE INFOPATHLEXE VISIOLEXE VPREVIEWLEXE LYNKLEXE PPTVIEWLEXE	X X	×		Heap	EAF	EAF+	Mand	Botto	d.bea1	MemP	Caller	SmEx	Stadk	ASR	
INFOPATHLEXE VISIOLEXE VPREVIEW.EXE LYIKC.EXE PPTVIEW.EXE	2		4	2	~	0	1	2	2	V	V	V	4	100	A
VISIOLEXE VPREVIEW.EXE LYIKC.EXE PPTVIEW.EXE		1	V	4	2	D	V	2	~	1	V	2	~	T	
VPREVIEW.EXE LYNC.EXE PPTVIEW.EXE	×	4	4	4	4	1.0	4	~	~	~	~	4	4		
LYNC-EXE PPTVIEW.EXE		4	1	9	2	0	2	9	9	1	9	9	1	TO	
PPTV1EW.EXE	8	2	2	8	2	0	2	8	8	2	R	2	2	17	
	1	~	1	4	V.		1	~	~	2	~	~	2	1 13	F
OIS.EXE	2	1	1	1	4	I EI	4	4	4	1	~	2	1		
AcroRd32.exe	8	~	1	8	1	1	2	2	9	2	8	8	V		
Acrobat.exe	1	1	~	1	9	4	~	~	8	2	~	2	×		
java.exe	1	1	8	10	2	0	1	1	8	4	8	4	4	E	
javaw.exe	4	1	$\mathbf{\mathbf{r}}$	1.8	1	2	4	4	8	×.	2	4	Y		
javaws.exe	×.	*	×.		1		×	1	1	1	1	8	4		6
dent.exe	2	1	2	×			1	2	1	1	8	2	~		
chiph.exe	8	8	8	4	×.		1	8	1	8	4	2	1		
CyberGhost.exe	1	×		8	2	1.0	8	8	9	2	8	9	1		
Connectify.exe	8	8	1	8	2		2	8	×	8	R	8	2	12	
wfc.exe	×	×	~	1	2	1 0	~	2	1	1	2	1	1		1

Spätestens an dieser Stelle wird es Zeit sich mit dem EMET Benutzerhandbuch zu beschäftigen.